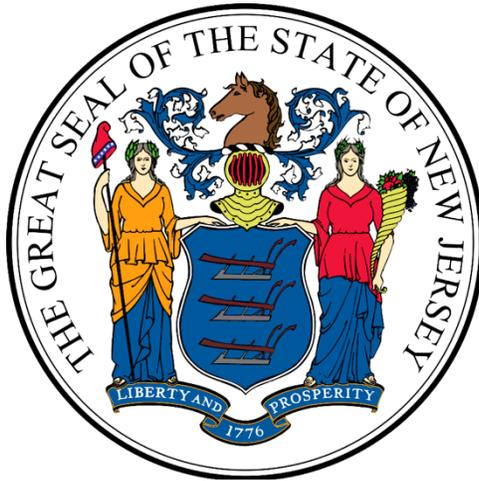


# **Executive Branch of New Jersey State Government**



## **Statewide Information Security Manual**

**Published By: NJ Office of Homeland Security and Preparedness  
Effective Date: February 2, 2021**

---

## TABLE OF CONTENTS

---

<b>INFORMATION SECURITY AND PRIVACY PROGRAM (PM)</b> .....	<b>10</b>
PM-01: STATEWIDE INFORMATION SECURITY MANUAL PURPOSE .....	11
PM-02: AUTHORITY .....	12
PM-03: SCOPE AND APPLICABILITY .....	13
PM-04: CYBERSECURITY AND PRIVACY BASELINE .....	13
PM-05: INFORMATION SECURITY AND PRIVACY RESOURCES .....	14
PM-06: ORGANIZATION OF THE STATEWIDE INFORMATION SECURITY MANUAL.....	14
PM-07: STATEWIDE INFORMATION SECURITY MANUAL CREATION AND MAINTENANCE .....	15
PM-08: POLICY AND STANDARDS DISTRIBUTION.....	16
PM-09: UPDATES.....	16
PM-10: SECURITY COMMUNICATION AND TRAINING .....	16
PM-11: ENFORCEMENT AND COMPLIANCE .....	17
<b>ORGANIZATIONAL SECURITY (OR)</b> .....	<b>18</b>
OR-01: PURPOSE .....	18
OR-02: POLICY .....	18
OR-03: INFORMATION SECURITY AND PRIVACY ROLES AND RESPONSIBILITIES .....	18
OR-04: INFORMATION SECURITY GOVERNANCE COMMITTEE (ISGC).....	18
OR-05: DIRECTOR, NEW JERSEY OFFICE OF HOMELAND SECURITY AND PREPAREDNESS .....	19
OR-06: STATE CHIEF TECHNOLOGY OFFICER (CTO) .....	19
OR-07: STATE CHIEF INFORMATION SECURITY OFFICER (CISO) .....	20
OR-08: DIRECTOR OF THE NJCCIC.....	21
OR-09: NEW JERSEY STATE PRIVACY OFFICER .....	22
OR-10: HEADS OF STATE AGENCIES.....	23
OR-11: AGENCY CHIEF INFORMATION OFFICER (CIO).....	23
OR-12: AGENCY CHIEF INFORMATION SECURITY OFFICER (CISO).....	24
OR-13: AGENCY PRIVACY OFFICER .....	25
OR-14: FUNCTIONAL ROLES AND RESPONSIBILITIES.....	25
OR-15: INFORMATION SYSTEM OWNER .....	25
OR-16: INFORMATION OWNER.....	26
OR-17: ASSET CUSTODIAN.....	26
OR-18: AGENCY HUMAN RESOURCES (HR) PERSONNEL .....	27
OR-19: OFFICE OF THE ATTORNEY GENERAL PERSONNEL.....	28
OR-20: USER .....	28
OR-21: SEPARATION OF DUTIES .....	29
OR-22: CONTACTS WITH EXTERNAL ORGANIZATIONS.....	30
OR-23: INDEPENDENT REVIEW OF INFORMATION SECURITY PROGRAM .....	30
OR-24: REPORTING OF INCIDENTS .....	30

<b>PERSONNEL SECURITY (PS)</b> .....	<b>32</b>
PS-01: PURPOSE .....	32
PS-02: POLICY .....	32
PS-03: POSITION RISK DESIGNATION .....	32
PS-04: PERSONNEL SCREENING.....	33
PS-05: TRANSFERS AND PROMOTIONS .....	33
PS-06: PERSONNEL TERMINATION.....	33
PS-07: ACCESS AGREEMENTS .....	34
PS-08: THIRD-PARTY PERSONNEL SECURITY .....	34
PS-09: RULES OF BEHAVIOR .....	35
PS-10: AGENCY REQUIREMENTS .....	35
PS-11: USER REQUIREMENTS .....	35
PS-12: INCIDENTAL USE OF STATE OF NEW JERSEY INFORMATION ASSETS.....	37
PS-13: REPORTING OF INCIDENTS .....	37
PS-14: NO EXPECTATION OF PRIVACY .....	38
PS-15: SECURITY MONITORING.....	38
PS-16: PERSONNEL SANCTIONS .....	38
<b>SECURITY AWARENESS AND TRAINING (AT)</b> .....	<b>40</b>
AT-01: PURPOSE .....	40
AT-02: POLICY.....	40
AT-03: INFORMATION SECURITY AND PRIVACY AWARENESS PROGRAM .....	40
AT-04: INFORMATION SECURITY AND PRIVACY TRAINING .....	41
AT-05: ROLE-BASED SECURITY AND PRIVACY TRAINING .....	42
AT-06: PRACTICAL EXERCISES.....	42
AT-07: TRAINING RECORDS .....	43
AT-08: SECURITY ADVISORIES AND ALERTS.....	43
AT-09: INFORMATION SECURITY RESOURCES.....	43
<b>RISK ASSESSMENT (RA)</b> .....	<b>44</b>
RA-01: PURPOSE.....	44
RA-02: RISK ASSESSMENT POLICY .....	45
RA-03: SECURITY CATEGORIZATION.....	45
RA-04: DATA CLASSIFICATION .....	46
RA-05: DATA CLASSIFICATION AND SECURITY CATEGORIZATION CONSIDERATIONS.....	46
RA-06: ASSIGNING SECURITY CATEGORIZATIONS .....	51
RA-07: RISK ASSESSMENTS.....	52
RA-08: SUPPLY CHAIN RISK ASSESSMENTS.....	53
RA-09: RISK ASSESSMENT COMPONENTS: .....	53
RA-10: RISK CONSIDERATIONS .....	55
RA-11: USE OF ALL-SOURCE INTELLIGENCE IN ASSESSING RISK .....	56
RA-12: VULNERABILITY MONITORING AND SCANNING .....	56
RA-13: VULNERABILITY AND PATCH MANAGEMENT .....	56

RA-14: VULNERABILITY SCANNING AND REMEDIATION .....	57
RA-15: SOFTWARE PATCHING AND CURRENCY .....	58
RA-16: RESPONSIBLE DISCLOSURE .....	58
RA-17: SECURITY TESTING AUTHORIZATION .....	58
RA-18: THREAT HUNTING.....	59
<b>PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY (PT) .....</b>	<b>60</b>
PT-01: PURPOSE .....	60
PT-02: POLICY .....	60
PT-03: PRIVACY PROGRAM .....	61
PT-04: DISSEMINATION OF PRIVACY PROGRAM INFORMATION .....	61
PT-05: AUTHORITY TO PROCESS PERSONALLY IDENTIFIABLE INFORMATION.....	62
PT-06: PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES.....	62
PT-07: CONSENT .....	62
PT-08: MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION .....	63
PT-09: PRIVACY NOTICE.....	63
PT-10: SPECIFIC CATEGORIES OF PERSONALLY IDENTIFIABLE INFORMATION .....	64
PT-11: PERSONALLY IDENTIFIABLE INFORMATION QUALITY MANAGEMENT .....	64
<b>MEDIA PROTECTION (MP) .....</b>	<b>66</b>
MP-01: PURPOSE.....	66
MP-02: POLICY .....	67
MP-03: MEDIA ACCESS.....	67
MP-04: MEDIA MARKING .....	67
MP-05: MEDIA STORAGE.....	67
MP-06: MEDIA TRANSPORT .....	68
MP-07: MEDIA USE.....	69
MP-08: PORTABLE STORAGE DEVICES.....	69
MP-09: MEDIA SANITIZATION .....	70
MP-10: RECORDS RETENTION .....	71
<b>CONFIGURATION MANAGEMENT (CM) .....</b>	<b>72</b>
CM-01: PURPOSE.....	72
CM-02: POLICY .....	72
CM-03: BASELINE CONFIGURATIONS.....	72
CM-04: CONFIGURATION CHANGE CONTROL.....	73
CM-05: IMPACT ANALYSIS.....	74
CM-06: ACCESS RESTRICTIONS FOR CHANGE.....	75
CM-07: CONFIGURATION SETTINGS.....	75
CM-08: LEAST FUNCTIONALITY .....	76
CM-09: SYSTEM COMPONENT INVENTORY .....	77
CM-10: CONFIGURATION MANAGEMENT PLAN.....	79
CM-11: SOFTWARE USAGE RESTRICTIONS.....	79

CM-12: USER INSTALLED SOFTWARE .....	80
CM-13: INFORMATION LOCATION .....	80
<b>ACCESS CONTROL (AC).....</b>	<b>82</b>
AC-01: PURPOSE.....	82
AC-02: POLICY.....	83
AC-03: ACCOUNT MANAGEMENT .....	83
AC-04: REQUIREMENTS FOR ACCOUNT REGISTRATION AND CREATION .....	85
AC-05: REQUIREMENTS FOR PRIVILEGED ACCESS.....	86
AC-06: REQUIREMENTS FOR TEMPORARY OR EMERGENCY ACCESS .....	86
AC-07: ACCESS ENFORCEMENT .....	87
AC-08: INFORMATION FLOW ENFORCEMENT.....	87
AC-09: SEPARATION OF DUTIES .....	88
AC-10: LEAST PRIVILEGE .....	88
AC-11: UNSUCCESSFUL LOGON ATTEMPTS.....	89
AC-12: HUMAN REVIEWS .....	90
AC-13: SYSTEM USE NOTIFICATION.....	91
AC-14: DEVICE LOCK .....	92
AC-15: SESSION TERMINATION .....	92
AC-16: PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION .....	93
AC-17: REMOTE ACCESS.....	93
AC-17.1: CENTRALIZED MANAGEMENT OF REMOTE ACCESS INFRASTRUCTURE .....	94
AC-17.2: REMOTE ACCESS SECURITY.....	95
AC-17.3: REMOTE ACCESS - AGENCY LEVEL AUTHORIZATION .....	97
AC-17.4: TRAINING OF REMOTE ACCESS USERS.....	97
AC-17.5: REMOTE ACCESS - USER RESPONSIBILITIES .....	97
AC-18: WIRELESS ACCESS .....	98
AC-19: USE OF EXTERNAL SYSTEMS.....	99
AC-20: MOBILE DEVICES.....	100
AC-20.1: AUTHORIZATION FOR USE OF MOBILE DEVICES.....	101
AC-20.2: MOBILE DEVICE RISK ASSESSMENT REQUIREMENT .....	101
AC-20.3: MOBILE DEVICE - BRING YOUR OWN DEVICE (BYOD) .....	102
AC-20.4: MOBILE DEVICE NETWORK ACCESS .....	102
AC-20.5: CENTRALIZED MANAGEMENT OF MOBILE DEVICES .....	103
AC-20.6: ELIGIBLE MOBILE DEVICES .....	103
AC-20.7: MOBILE DEVICE TECHNICAL SECURITY CONTROLS .....	104
AC-20.8: INVENTORY OF MOBILE DEVICES.....	105
AC-20.9: APPROVED APPLICATION STORES .....	105
AC-20.10: APPROVED APPLICATIONS.....	106
AC-20.11: APPLICATION MANAGEMENT .....	106
AC-20.12: APPROVED CLOUD SERVICES .....	106
AC-20.13: BACKUP.....	106
AC-20.14: SAFETY AND COMPLIANCE .....	107

AC-20.15: TRAINING OF MOBILE DEVICE USERS .....	107
AC-21: INFORMATION SHARING .....	107
AC-22: PUBLICLY ACCESSIBLE CONTENT .....	108
<b>IDENTITY AND AUTHENTICATION (IA).....</b>	<b>110</b>
IA-01: PURPOSE.....	110
IA-02: POLICY.....	110
IA-03: USER IDENTIFICATION AND AUTHENTICATION .....	110
IA-04: DEVICE IDENTIFICATION AND AUTHENTICATION .....	111
IA-05: IDENTIFIER MANAGEMENT .....	112
IA-06: AUTHENTICATOR MANAGEMENT .....	112
IA-07: PASSWORD-BASED AUTHENTICATION .....	113
IA-08: PASSWORD REQUIREMENTS FOR NON-PRIVILEGED USER ACCOUNTS.....	114
IA-09: PASSWORD REQUIREMENTS FOR PRIVILEGED USER ACCOUNTS.....	115
IA-10: PASSWORD REQUIREMENTS FOR SERVICE ACCOUNTS.....	116
IA-11: PUBLIC KEY-BASED AUTHENTICATION.....	117
IA-12: PROTECTION OF AUTHENTICATORS .....	117
IA-13: AUTHENTICATION FEEDBACK.....	117
IA-14: CRYPTOGRAPHIC MODULE AUTHENTICATION.....	118
IA-15: IDENTIFICATION AND AUTHENTICATION FOR EXTERNAL USERS.....	118
IA-16: RE-AUTHENTICATION .....	118
IA-17: IDENTITY PROOFING .....	119
<b>SYSTEM AND INFORMATION INTEGRITY (SI).....</b>	<b>121</b>
SI-01: PURPOSE .....	121
SI-02: POLICY .....	121
SI-03: FLAW REMEDIATION .....	122
SI-04: MALICIOUS CODE PROTECTION .....	122
SI-05: SYSTEM MONITORING .....	123
SI-06: SECURITY ALERTS, ADVISORIES AND DIRECTIVES.....	123
SI-07: SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY .....	124
SI-08: EMAIL AND WEB FILTERING PROTECTION .....	124
SI-09: INFORMATION INPUT VALIDATION.....	125
SI-10: ERROR HANDLING .....	125
SI-11: MEMORY PROTECTION .....	125
SI-12: INFORMATION MANAGEMENT AND RETENTION .....	126
SI-13: PERSONALLY IDENTIFIABLE INFORMATION .....	126
<b>SYSTEM AND COMMUNICATIONS PROTECTION (SC) .....</b>	<b>128</b>
SC-01: PURPOSE .....	128
SC-02: POLICY .....	128
SC-03: IDENTIFIED RESPONSIBILITY.....	129
SC-04: SEPARATION OF SYSTEM AND USER FUNCTIONALITY.....	129

SC-05: INFORMATION IN SHARED SYSTEM RESOURCES .....	129
SC-06: DENIAL-OF-SERVICE PROTECTION .....	130
SC-07: BOUNDARY PROTECTION .....	131
SC-07.1: ACCESS POINTS .....	131
SC-07.2: EXTERNAL TELECOMMUNICATIONS/DATA SERVICES .....	132
SC-07.3: DENY BY DEFAULT/ALLOW BY EXCEPTION .....	132
SC-07.4: SPLIT TUNNELING FOR REMOTE DEVICES .....	132
SC-07.5: PROXY SERVERS.....	133
SC-07.6: PREVENT EXFILTRATION/DATA LOSS PREVENTION .....	133
SC-07.7: HOST BASED PROTECTION .....	134
SC-08: TRANSMISSION CONFIDENTIALITY AND INTEGRITY.....	134
SC-09: NETWORK DISCONNECT.....	134
SC-10: CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT .....	135
SC-11: CRYPTOGRAPHIC PROTECTION .....	135
SC-11.1: DATA AT REST .....	136
SC-11.2: DATA IN TRANSIT.....	136
SC-11.3: PUBLICLY ACCESSIBLE WEBSITE AND SERVICES: .....	136
SC-12: COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS .....	137
SC-13: PUBLIC KEY INFRASTRUCTURE CERTIFICATES .....	137
SC-14: MOBILE CODE.....	137
SC-15: SECURE NAME/ADDRESS RESOLUTION SERVICE .....	137
SC-16: ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE .....	138
SC-17: SESSION AUTHENTICITY .....	139
SC-18: PROCESS ISOLATION .....	140
SC-19: USAGE RESTRICTIONS .....	140
SC-20: DETONATION CHAMBERS .....	140
<b>SYSTEM AND SERVICES ACQUISITION (SA).....</b>	<b>142</b>
SA-01: PURPOSE .....	142
SA-02: POLICY .....	142
SA-03: ALLOCATION OF RESOURCES .....	143
SA-04: SYSTEM DEVELOPMENT LIFE CYCLE .....	143
SA-05: ACQUISITION PROCESS .....	144
SA-06: SYSTEM DOCUMENTATION .....	146
SA-07: SECURITY AND PRIVACY ENGINEERING PRINCIPLES .....	147
SA-08: EXTERNAL SYSTEM SERVICES .....	148
SA-09: DEVELOPER CONFIGURATION MANAGEMENT .....	148
SA-10: DEVELOPER TESTING AND EVALUATION.....	149
SA-11: DEVELOPMENT PROCESS, STANDARDS, AND TOOLS.....	150
SA-12: DEVELOPER-PROVIDED TRAINING .....	151
SA-13: DEVELOPER SCREENING.....	152
SA-14: UNSUPPORTED SYSTEM COMPONENTS .....	152

<b>SUPPLY CHAIN RISK MANAGEMENT (SU)</b> .....	<b>154</b>
SU-01: PURPOSE.....	154
SU-02: POLICY.....	154
SU-03: SUPPLY CHAIN RISK MANAGEMENT PLAN.....	154
SU-04: SUPPLY CHAIN CONTROLS AND PROCESSES.....	155
SU-05: ACQUISITION STRATEGIES, TOOLS, AND METHODS.....	156
SU-06: SUPPLIER ASSESSMENTS AND REVIEWS.....	156
SU-07: NOTIFICATION AGREEMENTS.....	157
SU-08: INSPECTION OF SYSTEMS OR COMPONENTS.....	157
SU-09: COMPONENT AUTHENTICITY.....	157
SU-10: COMPONENT DISPOSAL.....	158
<b>ASSESSMENT, AUTHORIZATION, AND MONITORING (CA)</b> .....	<b>160</b>
CA-01: PURPOSE.....	160
CA-02: POLICY.....	161
CA-03: CONTROL ASSESSMENTS.....	161
CA-04: INFORMATION EXCHANGE.....	161
CA-05: PLAN OF ACTION AND MILESTONES.....	162
CA-06: AUTHORIZATION.....	162
CA-07: CONTINUOUS MONITORING.....	163
CA-08: PENETRATION TESTING AND RED TEAM EXERCISES.....	163
CA-09: INTERNAL SYSTEM CONNECTIONS.....	164
<b>AUDIT AND ACCOUNTABILITY (AU)</b> .....	<b>165</b>
AU-01: PURPOSE.....	165
AU-02: POLICY.....	165
AU-03: AUDIT EVENTS.....	166
AU-04: CONTENT OF AUDIT RECORDS.....	166
AU-05: PERSONALLY IDENTIFIABLE INFORMATION IN AUDIT LOGS.....	168
AU-06: AUDIT LOG STORAGE CAPACITY.....	168
AU-07: RESPONSE TO AUDIT LOGGING PROCESS FAILURES.....	168
AU-08: AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING.....	168
AU-09: AUDIT REDUCTION AND REPORT GENERATION.....	169
AU-10: TIME STAMPS.....	169
AU-11: PROTECTION OF AUDIT RECORDS.....	169
<b>MAINTENANCE (MA)</b> .....	<b>171</b>
MA-01: PURPOSE.....	171
MA-02: POLICY.....	171
MA-03: CONTROLLED MAINTENANCE.....	171
MA-04: MAINTENANCE TOOLS.....	172
MA-05: NONLOCAL MAINTENANCE.....	173
MA-06: MAINTENANCE PERSONNEL.....	173

<b>PLANNING (PL)</b> .....	<b>175</b>
PL-01: PURPOSE .....	175
PL-02: POLICY .....	175
PL-03: SYSTEM SECURITY AND PRIVACY PLAN .....	175
PL-04: COMPLETION AND SUBMISSION OF THE SYSTEM SECURITY AND PRIVACY PLAN.....	176
PL-05: RULES OF BEHAVIOR.....	176
PL-05.1: AGENCY RESPONSIBILITIES.....	177
PL-05.2: USER REQUIREMENTS .....	177
PL-06: SECURITY AND PRIVACY ARCHITECTURE .....	179
PL-07: CENTRAL MANAGEMENT .....	180
PL-08: BASELINE SELECTION.....	181
PL-09: EXCEPTIONS TO BASELINE CONTROLS.....	181
PL-09.1: DOCUMENT EXCEPTION .....	181
PL-09.2: REQUEST APPROVAL .....	182
<b>PHYSICAL AND ENVIRONMENTAL SECURITY (PE)</b> .....	<b>184</b>
PE-01: PURPOSE .....	184
PE-02: POLICY .....	184
PE-03: PHYSICAL ACCESS SECURITY ZONES .....	184
PE-04: PHYSICAL ACCESS AUTHORIZATIONS .....	185
PE-05: VISITOR CONTROL .....	186
PE-06: LOST OR STOLEN ID BADGES .....	186
PE-07: PHYSICAL ACCESS CONTROLS.....	186
PE-08: SECURITY MONITORING AND AUDITING OF PHYSICAL ACCESS .....	187
PE-09: RETENTION OF SECURITY LOGS AND VIDEO.....	187
PE-10: CLEAN DESK/CLEAN SCREEN REQUIREMENTS .....	188
PE-11: POWER EQUIPMENT AND POWER CABLING .....	188
PE-12: EMERGENCY SHUTOFF .....	188
PE-13: EMERGENCY POWER.....	188
PE-14: EMERGENCY LIGHTING .....	188
PE-15: FIRE PROTECTION.....	188
PE-16: TEMPERATURE AND HUMIDITY CONTROLS .....	189
PE-17: WATER DAMAGE PROTECTION .....	189
PE-18: ALTERNATE WORK SITE .....	189
PE-19: DELIVERY AND REMOVAL OF INFORMATION ASSETS .....	189
PE-20: SECURING PORTABLE INFORMATION ASSETS.....	189
PE-21: DISPOSAL/TRANSFER OF INFORMATION ASSETS.....	190
<b>CONTINGENCY PLANNING (CP)</b> .....	<b>191</b>
CP-01: PURPOSE .....	191
CP-02: POLICY.....	191
CP-03: CONTINGENCY PLAN .....	191

CP-04: CONTINGENCY TRAINING .....	193
CP-05: CONTINGENCY PLAN TESTING .....	193
CP-06: ALTERNATE STORAGE SITE.....	194
CP-07: ALTERNATE PROCESSING SITE .....	194
CP-08: TELECOMMUNICATIONS SERVICES.....	194
CP-09: SYSTEM BACKUP .....	195
CP-10: SYSTEM RECOVERY AND RECONSTITUION.....	196
<b>INCIDENT RESPONSE (IR) .....</b>	<b>197</b>
IR-01: PURPOSE .....	197
IR-02: POLICY.....	197
IR-03: REPORTING INFORMATION SECURITY AND PRIVACY INCIDENTS .....	197
IR-04: INCIDENT RESPONSE PLANNING .....	198
IR-05: INCIDENT RESPONSE TRAINING .....	198
IR-06: INCIDENT RESPONSE TESTING .....	199
IR-07: INCIDENT RESPONSE TEAM .....	199
IR-08: SIGNIFICANT CYBERSECURITY INCIDENTS.....	200
IR-09: INCIDENT CATEGORIZATION .....	201
IR-10: INCIDENT SEVERITY AND PRIORITIZATION.....	202
IR-11: INCIDENT TRACKING, DOCUMENTATION, AND REPORTS.....	202
<b>APPENDIX A – GLOSSARY OF KEY TERMS .....</b>	<b>204</b>
<b>APPENDIX B – NJCCIC CYBERSECURITY GUIDELINES FOR INTERNATIONAL TRAVEL .....</b>	<b>326</b>
<b>APPENDIX C - RECORD OF CHANGES .....</b>	<b>328</b>

---

## INFORMATION SECURITY AND PRIVACY PROGRAM (PM)

---

The State of New Jersey affirms the fundamental significance of information security by delineating a set of policies and standards to securely protect the Executive Branch of New Jersey State Government information and information systems, while maintaining compliance with State and Federal laws, executive orders, regulatory, contractual, and other policy requirements pertaining to confidentiality, integrity, availability, privacy, and safety. New Jersey State Government departments and agencies act as the custodians of extensive information holdings and rely upon information systems for fiscal, policy, and program delivery initiatives. Consequently, security and privacy measures must be implemented to guard against unauthorized access to, alteration, disclosure, or destruction of information and information systems, and safeguards must be implemented to offset possible threats.

The information security policies, standards, processes, and supplemental guidance contained in the Statewide Information Security Manual are key components of the State's information security program. Five information security objectives: Confidentiality, Integrity, Availability, Privacy, and Safety comprise its foundation.

- **Confidentiality** The property that sensitive information is not disclosed to unauthorized individuals, entities, or processes.
- **Integrity** - The property that sensitive information is not been modified or deleted in an unauthorized and undetected manner.
- **Availability** - The property that information or an information system is accessible and useable upon demand by an authorized entity.
- **Privacy** - The freedom from unauthorized intrusion or disclosure of information about an individual.
- **Safety** - The condition of being protected from harm or other non-desirable outcomes.

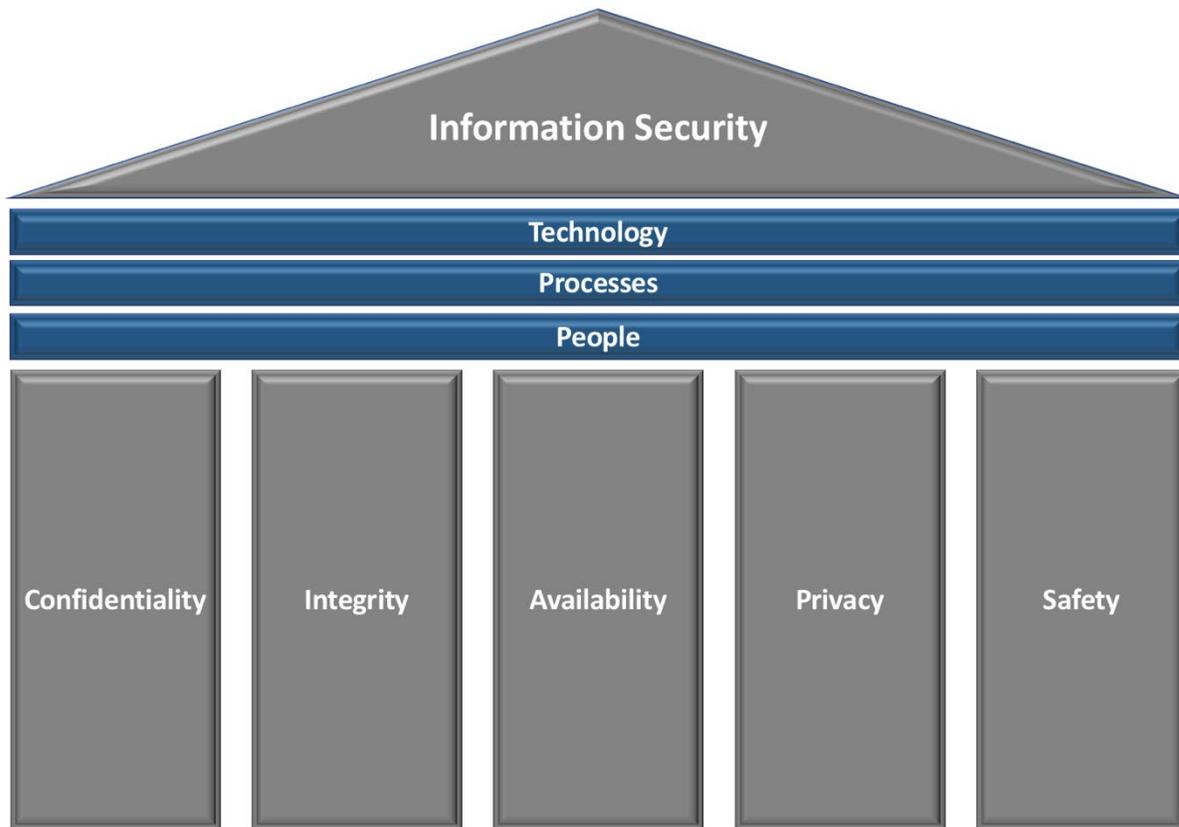


Figure 1 - Cybersecurity Objectives

These information security objectives can only be achieved if organizations embed them into their people, processes, and technology.

- **People** - Security is implemented and practiced by people. People design and implement processes and technology, as well as follow processes and use technology to enable business.
- **Processes** - Include formal and informal mechanisms (large and small, simple and complex) to accomplish objectives. Processes identify, measure, manage, and control risks to confidentiality, integrity, availability, privacy, and safety, and they also ensure accountability.
- **Technology** - Composed of the tools, applications, and infrastructure that make processes more efficient. Technology implemented by people following processes allows for the State to meet its information security objectives.

## PM-01: STATEWIDE INFORMATION SECURITY MANUAL PURPOSE

The purpose of the Executive Branch of New Jersey State Government’s Statewide Information Security Manual, hereinafter referred to as the Manual, is to assist New Jersey State Government organizations in applying a risk–based approach to information security while establishing the

required behaviors and controls necessary to protect information technology resources, secure personal information, safeguard privacy, and maintain the physical safety of individuals.

This Manual includes a set of policies and standards that sets a clear direction for information security and its role in supporting Executive Branch departments and agencies in their efforts to carry out their respective missions and to achieve their business goals and objectives, while effectively managing risk and ensuring the confidentiality, integrity and availability of their information and information systems. This Manual provides direction to the State workforce regarding their roles and responsibilities with respect to the security of State information assets. The implementation of consistent security controls across the Executive Branch of New Jersey State Government will help departments and agencies comply with current and future legal obligations to ensure due diligence in protecting the confidentiality, integrity, availability, privacy, and safety of State information and information systems.

The Executive Branch of New Jersey State Government's Statewide Information Security Manual has been derived from applicable State and Federal laws; industry best practices, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework for Improving Critical Infrastructure, NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations; lessons learned; and other New Jersey State Government business and technology related considerations.

This Manual is intended to provide State agencies with a means to tailor cost-effective security controls necessary to protect the confidentiality, integrity, availability, and privacy of State information and information systems commensurate with their sensitivity and criticality, while also maintaining and ensuring compliance with all legal requirements.

## **PM-02: AUTHORITY**

The policies, standards, and guidelines included in the Executive Branch of New Jersey State Government's Statewide Information Security Manual are established under the authority of:

- New Jersey Executive Order No. 5 creating the Office of Homeland Security and Preparedness (OHSP) (Corzine, 3/6/2006);
- New Jersey Executive Order No. 178 creating the New Jersey Cybersecurity and Communications Integration Cell ("NJCCIC") (Christie, 5/20/2015);
- Domestic Security Preparedness Act, P.L. 2001, C.246;
- The Critical Infrastructure Information Act of 2002, 6 U.S.C. § 133 et seq.; and
- N.J.S.A., Sections C.52:18A-224 through C.52:18A-234, The Office of Information Technology Reorganization Act.

The Information Security Policies and Standards are supported at the highest levels of the Executive Branch of New Jersey State Government.

## **PM-03: SCOPE AND APPLICABILITY**

The policies, standards, procedures, and guidelines included in the Statewide Information Security Manual apply to all Departments, Agencies, Commissions, Boards, Bodies, or other instrumentalities of the Executive Branch of New Jersey State Government, hereinafter referred to as: agencies, the Executive Branch, the SoNJ, or the State. All Executive Branch full-time and part-time employees, temporary workers, volunteers, interns, contractors, and those employed by contracted entities - collectively referred to as users - are governed by and responsible for complying with the policies and standards regardless of agency, location, or role.

This Manual applies to all information assets owned, leased, licensed, managed, or used by Executive Branch agencies, their business partners, contractors, and other authorized third parties on behalf of the State of New Jersey. Information assets include, but are not limited to, all information, data, devices, hardware (e.g. servers, laptop and desktop computers, tablets, phones, switches, etc.), software (e.g. commercial off-the-shelf and custom developed applications and support systems), services, or other components of information or communications systems.

The policies, standards, procedures, and guidelines included in this Manual supersede any previous Executive Branch Statewide information security policies, standards, procedures, and guidelines issued prior to February 2, 2021, the effective date. These policies, standards, procedures, and guidelines have been written in conformance with and do not supersede any applicable State or Federal laws, executive orders, circulars, or existing contracts, memorandums of understanding, or labor management agreements in effect as of the effective date of the Statewide Information Security Manual.

## **PM-04: CYBERSECURITY AND PRIVACY BASELINE**

Individual agencies have various legal, regulatory, and contractual compliance requirements based on their business services and operations, and the information they collect, store, process, and transmit. Some commonly applicable statutory and regulatory requirements include [IRS Publication 1075, Safeguards for Protecting Federal Tax Returns and Return Information](#), Health Insurance Portability and Accountability Act (HIPAA), [Minimum Acceptable Risk Standards for Exchanges, version 2.0 \(MARS-E\)](#), [Family Education Rights Privacy Act \(FERPA\)](#), [Payment Card Industry – Data Security Standards \(PCI-DSS\)](#), [Criminal Justice Information Services \(CJIS\)](#), [European Union General Data Protection Regulation \(GDPR\)](#), [California Consumer Privacy Act \(CCPA\)](#), [Children’s Online Privacy Protection Act \(COPPA\)](#) and others. In order to satisfy the control objectives for the above statutory and regulatory requirements, and to provide a uniform baseline, all State-owned, leased, licensed, or managed information systems, system components, and system services are required to, at a minimum, implement Moderate level controls as defined by [NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations](#).

Agencies may develop and implement a more restrictive set of information security policies and standards for use within their respective organization or for a specific information system,

program, or requirement. Agency-developed information security policies and standards can exceed, but must not conflict with, the baseline established by this Manual.

The Executive Branch of New Jersey State Government's Statewide Information Security Manual does not apply to independent State entities that are not subject to the policy supervision and control of the Governor. Examples of independent State entities include the New Jersey Transit Authority, the New Jersey Turnpike Authority, etc.

## **PM-05: INFORMATION SECURITY AND PRIVACY RESOURCES**

In order to ensure the resources necessary to appropriately manage information security and privacy risks in accordance with the policies, standards, processes, and guidelines included in this manual, agencies are required to:

- (a) Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement;
- (b) Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, circulars, directives, policies, regulations, standards; and
- (c) Make available for expenditure, the planned information security and privacy resources.

Supplemental Guidance: In addition to individual agencies budgeting and allocating information security and privacy resources, the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) and the New Jersey Office of Information Technology (NJOIT) also plan, budget for, and provide resources to all agencies in the Executive Branch of New Jersey State Government. Agencies Are encouraged to contact both the NJCCIC and NJOIT for more information of available resources.

## **PM-06: ORGANIZATION OF THE STATEWIDE INFORMATION SECURITY MANUAL**

The individual information security policies, standards, procedures, and guidelines, along with their supporting references and forms, have been compiled and organized into the Executive Branch of New Jersey State Government's Statewide Information Security Manual as each policy, standard, and guideline presented has key dependencies with others. The collection of policies, standards, procedures, and guidelines organized within this Manual provides context, consistency, and clarity, whereas separate policies and standards may lead to gaps, inconsistencies, and conflicts.

The sections of this Manual are organized to generally align with the control families that can be found in [NIST Special Publication 800-53 Revision 5](#). The controls included in this Manual are tailored to New Jersey State government in order to allow for continuous business and service enablement through intelligent risk management.

The information security documentation in this Manual is comprised of four (4) main components:

- **Policy** - Documents high-level rules, establishes roles and responsibilities, and sets management expectations governing security practices, operational procedures, and the acceptable use of State information assets. Policies are supported by standards and further implemented by procedures.
- **Standard** - A mandatory control that helps enforce and support a policy. Standards include specifications for processes, practices, uses, and hardware and software configurations that are considered industry or government approved specifications. External standards organizations, such as the National Institute of Standards and Technology, the Center for Internet Security, and others publish approved information security standards that are included in this Manual.
- **Procedure** - Contains detailed descriptions of the steps necessary to perform specific operations in conformance with applicable standards and represent the implementation of a policy. They are generally developed by those who are responsible for the implementation of a policy or standard, such as systems administrators, network administrators, database administrators, etc.
- **Supplemental Guideline** - Consists of recommendations, best practices, and supporting documents and processes that help with the interpretation and implementation of a specific policy or standard. Supplemental Guidance is intended to help agencies and individuals to achieve a policy's objectives by providing a framework in order to implement procedures while allowing for discretion in their interpretation, implementation, or use. Supplemental Guidance may include background information regarding the policy, standards, and control objectives.

When applied in concert, they allow for security objectives to be achieved.

## **PM-07: STATEWIDE INFORMATION SECURITY MANUAL CREATION AND MAINTENANCE**

The State Chief Information Security Officer (CISO), within the New Jersey Office of Homeland Security and Preparedness' New Jersey Cybersecurity and Communications Integration Cell, has overall responsibility for the creation and maintenance of the Executive Branch of New Jersey State Government's Statewide Information Security Manual.

The policies, standards, procedures, and guidelines contained in this Manual shall be reviewed and approved at least annually by the CISO, under the oversight of the Information Security Governance Committee, to ensure the State's security program is relevant and applicable to manage the risks associated with new and emerging security threats and vulnerabilities as they arise.

Reviews of the Manual must also be initiated under the following circumstances:

- (a) In response to legislative, regulatory, or policy changes that have information security implications;
- (b) When industry, national, or international standards for information security are introduced or significantly revised to address emerging business and technology issues;
- (c) In response to a security risk assessment or audit in which the current controls are deemed to expose the State to unacceptable risks;
- (d) In response to threat or vulnerability trends that indicate State information and information systems are at significantly increased risk;
- (e) After the review of a significant information security incident; and/or
- (f) To account for the planning and implementation of new or significantly changed technologies.

The Manual is considered a living document and, as such, is subject to changes and modifications, with or without notification, as necessary to protect the State's business objectives, individuals, and assets. The State reserves the right to revoke, change, or supplement these policies, standards, procedures, and guidelines at any time without prior notice. Such changes shall be effective immediately upon approval by the State CISO, unless otherwise stated.

## **PM-08: POLICY AND STANDARDS DISTRIBUTION**

The State CISO is responsible for the creation and distribution of the Statewide Information Security Manual to all agencies. At a minimum, the contents of the Manual shall be distributed for viewing on agency Intranet websites.

## **PM-09: UPDATES**

Substantive changes or updates to the Manual will be announced to employees via email and/or announced on the NJCCIC website, [cyber.nj.gov](http://cyber.nj.gov). Changes will be noted in the [Record of Changes, Appendix C](#).

## **PM-10: SECURITY COMMUNICATION AND TRAINING**

Executive Branch agencies shall ensure that all users are familiar with the requirements of the Executive Branch of New Jersey State Government's Statewide Information Security Manual. Agencies shall conduct security awareness training for all users at least annually, to ensure that all personnel are aware of the security and privacy risks associated with their roles and that they understand their responsibilities, as well as applicable laws, policies, standards, and procedures related to the security of State information and information systems. New hires are required to complete information security awareness training within thirty (30) business days of their start date, as part of the required new hire training curriculum.

Agencies shall ensure that all interns, temporary workers, and contracted third parties covered by the Manual are familiar with it and comply with its requirements.

Users will be kept abreast of policy and standard changes via the following communication methods:

- Emails;
- State Internet sites;
- Department and Agency Intranet sites;
- Staff meetings;
- Annual security awareness training; and/or
- Other communications mediums as required.

## **PM-11: ENFORCEMENT AND COMPLIANCE**

All users of Executive Branch of New Jersey State Government information and information systems are governed by, and are responsible for, complying with the policies and standards in this Manual. Users who are found in violation of the information security and privacy policies and standards are subject to disciplinary action up to and including termination of employment, or immediate termination of contractor and/or vendor relationship. Violations of law may be referred to the appropriate law enforcement agency for investigation and prosecution.

## **PM-12: QUESTIONS**

Questions about this Manual may be directed to your respective Agency Chief Information Security Officer or to the New Jersey Cybersecurity and Communications Integration Cell, via email at [njccic@cyber.nj.gov](mailto:njccic@cyber.nj.gov).

## **REFERENCES**

The requirements established in the Program Management policies and standards have been derived from the following:

- NIST SP 800-53r5 Program Management (PM); and
- NIST CSF Identify/Governance (ID.GV).

---

## **ORGANIZATIONAL SECURITY (OR)**

---

### **OR-01: PURPOSE**

The purpose of the Organizational Security Policy is to establish and maintain a management framework that promotes and oversees the implementation of security controls and the performance of information security throughout the Executive Branch of New Jersey State Government.

### **KEY TERMS**

None. See the [Glossary](#) in Appendix A for complete listing of terms.

### **OR-02: POLICY**

The Chief Technology Officer (CTO) of New Jersey and the Director, New Jersey Office of Homeland Security and Preparedness (NJOHSP) jointly establish the Information Security Governance Committee and a management structure for information security across the Executive Branch of New Jersey State Government.

This policy incorporates the requirements from the State of New Jersey Office of Information Technology Circular, [Enterprise Information Security Governance and Management Policy, 17-03-NJOIT](#).

### **OR-03: INFORMATION SECURITY AND PRIVACY MANAGEMENT ROLES AND RESPONSIBILITIES**

The primary roles within the Executive Branch of the New Jersey State Government information security management framework as well as the responsibilities and expectations associated with these roles is as follows.

### **OR-04: INFORMATION SECURITY GOVERNANCE COMMITTEE (ISGC)**

The ISGC shall be established and co-chaired by the Director of NJOHSP and the Chief Technology Officer. Membership will include the State CISO, Director of the NJCCIC, as well as representatives from the Governor's Office, the Office of the Attorney General, the Civil Service Commission, the Department of the Treasury's Office of Management and Budget, and other State agencies, as appropriate. The ISGC shall report to the Cabinet and be responsible for:

- (a) Assisting the State CISO in overseeing and executing New Jersey's information security management program;
- (b) Reviewing the Statewide Information Security Policies and Standards—and subsequent amendments—to ensure their alignment with the Executive Branch of State Government business goals and objectives, risk tolerances, and statutory, regulatory, and contractual requirements;

- (c) Providing direction and counsel regarding the assessment and management of information security risks and cyber threats to the State of New Jersey;
- (d) Reviewing reports on major information security incidents and cases of non-compliance;
- (e) Overseeing the response to information security incidents;
- (f) Reviewing security metrics and trends regarding the overall performance of the information security program; and
- (g) Staying abreast of cybersecurity threats to the Executive Branch of State Government through briefings and reports.

### **OR-05: DIRECTOR, NEW JERSEY OFFICE OF HOMELAND SECURITY AND PREPAREDNESS**

The Director of NJOHSP shall administer, coordinate, lead, and supervise New Jersey's counter-terrorism and preparedness efforts. The goal of the Office of Homeland Security and Preparedness is to coordinate emergency response efforts across all levels of government, law enforcement, emergency management, non-profit organizations, other jurisdictions, and the private sector, to protect the people of New Jersey. In addition, the Director shall be responsible for the strategic development, execution, and management of an effective and efficient information security program to manage cyber risks and ensure the confidentiality, integrity, and availability of the Executive Branch's information assets. Additionally, the Director of NJOHSP shall:

- (a) Oversee the response to information security incidents;
- (b) Stay abreast of cybersecurity threats to the Executive Branch of State Government information and information systems; and
- (c) Advise the ISGC through regular briefings and reports.

### **OR-06: STATE CHIEF TECHNOLOGY OFFICER (CTO)**

The CTO leads NJOIT, which is responsible for providing and maintaining the information technology infrastructure of the Executive Branch of State Government, including all ancillary departments and agencies. The CTO provides vision and leadership for NJOIT and is responsible for coordinating and conducting all Executive Branch technology operations. The CTO directs the planning, implementation, and governance of enterprise Information Technology systems in support of the Executive Branch of State Government's business objectives and operations, to improve cost-effectiveness, service quality, and mission development.

At the CTO's direction, NJOIT fulfills the following responsibilities in support of the State's Information Security Program:

- (a) Design, acquisition, and implementation of enterprise IT systems in compliance with the Statewide Information Security Manual's Policies and Standards set by the State CISO;

- (b) Operation and support of IT systems in compliance with approved security procedures, including, but not limited to:
  - 1. IT asset management;
  - 2. Malware protection;
  - 3. Patch management;
  - 4. Web proxying and Content filtering;
  - 5. Secure file exchange; and
  - 6. Data encryption;
- (c) Management of third parties providing managed information services to NJOIT and other State entities;
- (d) Identity and access management;
- (e) Disaster recovery planning and operations;
- (f) Providing recommendations on policy and control enhancements to NJOHSP's Division of Cybersecurity;
- (g) Monitoring NJOIT's IT environment to identify, contain, or eliminate unauthorized activity;
- (h) Assisting in implementing the Information Security Incident Response Plan;
- (i) Providing subject-matter expertise for technical issues regarding information security; and
- (j) Executing the day-to-day security management of enterprise information, systems, and solutions through the application of controls as defined within the Statewide Information Security Manual's Policies and Standards.

Supplemental Guidance: Consistent with [Executive Order 225](#), the Office of Information Technology is responsible for providing and maintaining the information technology infrastructure (compute, network, and storage) of the Executive Branch, including all ancillary departments and agencies of the Executive Branch. Within this Manual, the policies and standards require agencies to implement safeguards necessary to protect information assets against a loss of confidentiality, integrity, and availability. The term "agency" includes NJOIT and all ancillary departments and agencies.

## **OR-07: STATE CHIEF INFORMATION SECURITY OFFICER (CISO)**

The State CISO reports to the Director of NJOHSP and serves as head of NJOHSP's Division of Cybersecurity. The State CISO shall establish and manage an information security program to ensure the confidentiality, integrity, and availability of the State of New Jersey Executive Branch's information resources, systems, and services while promoting and protecting privacy and safety. The State CISO has overall responsibility for the development, implementation, and performance of the information security program by:

- (a) Setting strategic information security planning across the Executive Branch of State Government;
- (b) Publishing the Statewide Information Security Manual's Policies and Standards;
- (c) Developing, managing, and executing the statewide Information Security Incident Response Plan;
- (d) Identifying security requirements to limit the risks associated with identified Executive Branch business objectives as defined by the Governor and the Heads of State agencies;
- (e) Developing, maintaining, and interpreting the Statewide Information Security Manual's Policies and Standards;
- (f) Providing information security subject matter expertise to State agencies;
- (g) Drafting and implementing an information security awareness and training program to be used by all State agencies;
- (h) Providing security metrics to track the performance of the information security program; and
- (i) Developing an Information Security Governance, Risk, and Compliance program, including, but not limited to:
  - 1. Coordinating and conducting compliance and risk assessments of agencies and their information assets;
  - 2. Conducting and managing vulnerability assessments of agency networks, applications, databases, and systems;
  - 3. Conducting penetration tests of agency networks, applications, databases, and systems; and
  - 4. Conducting information security risk assessments of third parties with access to State of New Jersey information assets.

## **OR-08: DIRECTOR OF THE NEW JERSEY CYBERSECURITY COMMUNICATIONS AND INTEGRATION CELL (NJCCIC)**

The NJCCIC, established within NJOHSP's Division of Cybersecurity, shall be the State's Cybersecurity Information Sharing and Analysis Organization. The Director of the NJCCIC shall be responsible for:

- (a) Developing and managing a cybersecurity information sharing and analysis organization to liaise with the National Cybersecurity and Communications Integration Center within the US Department of Homeland Security, other federal agencies, and other public and private sector entities on issues relating to cybersecurity;
- (b) Coordinating cybersecurity information sharing, performing cybersecurity threat analysis, and promoting shared and real-time situational awareness between and among the public and private sectors;

- (c) Coordinating information sharing related to cybersecurity risks, warnings, and incidents, and providing support on cybersecurity incident response and cybercrime investigations;
- (d) Providing information and recommending best practices on cybersecurity and resilience measures to public and private entities, including on information security and data protection;
- (e) Developing and implementing a cybersecurity threat information exchange with appropriate sources, including public utilities and private industry;
- (f) Implementing and monitoring a centralized Security Information and Event Management (SIEM) system and, where appropriate, identifying, containing, or eliminating unauthorized activity and other cyber threats;
- (g) Developing and managing an incident reporting system;
- (h) Developing and providing information security incident response assistance and subject-matter expertise, as required;
- (i) Providing cyber threat intelligence reports, analysis reports, briefings, alerts, and trainings to private and public organizations; and
- (j) Developing working relationships with external organizations, including law enforcement, the private sector, academia, Information Sharing and Analysis Organizations, Information Sharing and Analysis Centers, and regulatory authorities.

## **OR-09: NEW JERSEY STATE PRIVACY OFFICER**

The New Jersey State Privacy Officer reports to the State CTO and serves as the central point of guidance, leadership, vision, coordination and oversight of agency privacy programs.

At the CTO's direction, the State Privacy Officer coordinates the planning, implementation, governance and management of enterprise privacy initiatives and is responsible for the oversight of the State's compliance with all applicable State and Federal laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information.

The State Privacy Officer:

- (a) Ensures that the public has access to information about the State's privacy activities and can communicate with its officials for privacy;
- (b) Ensures that the State's privacy practices and reports are publicly available; and
- (c) Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.

## **OR-10: HEADS OF STATE AGENCIES (INCLUDES SECRETARIES, DIRECTORS, COMMISSIONERS, CHAIRPERSONS, OR EQUIVALENT HEAD OF A STATE ENTITY WITHIN THE EXECUTIVE BRANCH OF STATE GOVERNMENT)**

Heads of State Agencies (includes Secretaries, Directors, Commissioners, Chairpersons, or equivalent head of a state entity within the Executive Branch of State Government) are responsible for their respective agency's operations. Likewise, they are responsible for the overall protection and use of information assets owned, managed, or licensed by the agency. To these ends, they are charged with:

- (a) Driving commitment and support for the information security program;
- (b) Accepting risk on behalf of the agency;
- (c) Assigning appropriate IT management responsibilities within their respective agency to a designee who has the responsibility for the implementation and management of information technology systems in support of agency goals and objectives, and in accordance with the Executive Branch of State Government's Statewide Information Security Policies and Standards;
- (d) Assigning appropriate responsibilities within their agency to a designee who has the authority and responsibility for ensuring the implementation of, and the adherence to, the Information Security Program; and
- (e) Promoting adherence to information security policies and cyber awareness programs.

## **OR-11: AGENCY CHIEF INFORMATION OFFICER (CIO)**

The Agency CIO shall be responsible for the direction, planning, and implementation of information technology systems in support of agency business goals and objectives. In accordance with the New Jersey Office of Information Technology standards, directives and enterprise information strategy, the Agency CIO directs the planning and implementation of the agency information technology systems.

The Agency CIO fulfills the following responsibilities in support of the State's Information Security Program:

- (a) Design, acquisition, implementation, and operation of IT systems in compliance with approved policies and standards;
- (b) Operation/Support of IT systems in compliance with approved security procedures, including, but not limited to:
  - 1. IT asset management;
  - 2. Malware protection;
  - 3. Patch management; and
  - 4. Data encryption;

- (c) Management of third parties providing managed information services to the agency;
- (d) Identity and access management;
- (e) Disaster recovery planning and operations in coordination with NJOIT;
- (f) Providing recommendations regarding policy and control enhancements to the Division of Cybersecurity;
- (g) Monitoring the agency IT environment and, where appropriate, identifying, containing, and eliminating unauthorized activity;
- (h) Assisting in the implementation of the Information Security Incident Response Plan;
- (i) Executing the day-to-day security management of information, systems, and solutions through the application of controls as defined within the Statewide Information Security Manual's Policies and Standards; and
- (j) Providing subject matter expertise for technical issues regarding information security.

Supplemental Guidance: Consistent with [Executive Order 225](#), the Office of Information Technology is responsible for providing and maintaining the information technology infrastructure (compute, network, and storage) of the Executive Branch, including all ancillary departments and agencies of the Executive Branch. Within this Manual the policies and standards require agencies to implement safeguards necessary to protect information assets against a loss of confidentiality, integrity, and availability. The term "agency" includes NJOIT and all ancillary departments and agencies.

## **OR-12: AGENCY CHIEF INFORMATION SECURITY OFFICER (CISO)**

The Agency CISO shall be responsible for protecting and maintaining the confidentiality, integrity, and availability of information assets under his/her purview. The Agency CISO fulfills the following responsibilities in support of the Statewide Information Security Policies and Standards:

- (a) Identifying security requirements to effectively limit cyber risks associated with the agency's business goals and objectives;
- (b) Implementing and promoting information security awareness within their respective agency;
- (c) Ensuring compliance with the Statewide Information Security Manual's Policies and Standards within their respective State agency, including, but not limited to:
  1. Coordination of risk assessments and compliance audits with NJOHSP's Division of Cybersecurity;
  2. Coordination of vulnerability assessments of agency networks, applications, databases, and systems; and
  3. Coordination of risk assessments of third parties having access to agency information assets;
- (d) Assisting in the implementation of the Information Security Incident Response Plan; and

- (e) Reporting all information security incidents to the NJCCIC.

### **OR-13: AGENCY PRIVACY OFFICER**

Individual who is responsible for the oversight of the agency's compliance with all applicable State and Federal laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information.

### **OR-14: FUNCTIONAL ROLES AND RESPONSIBILITIES**

In addition to the management structure as documented above, the implementation and support for the State's information security program requires agencies to identify and assign appropriate personnel to the following functional roles and responsibilities.

### **OR-15: INFORMATION SYSTEM OWNER**

The information system owner is the agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. The information system owner may also be referred to as the Asset Owner. The information system owner has the following responsibilities related to system security:

- (a) Assigns the security categorization and criticality of the information system;
- (b) In coordination with the information owner, asset custodians, and stakeholders, develops and maintains security plans and contingency plans for all general support systems and major applications under their responsibility, including documenting the business associations and dependencies of the system (e.g., linked IT resources and flows of information);
- (c) Ensures contracts pertaining to the information system include provisions for necessary security and privacy controls;
- (d) Ensures that the information system is deployed and operated in accordance with the System Security and Privacy Plan and all applicable statutory, regulatory, contractual and policy requirements;
- (e) Ensures that access to sensitive information is limited to those with a "need to know" or "need to use";
- (f) Ensures the system's personnel are properly designated, monitored, and trained;
- (g) Ensures the system's users receive the requisite security training;
- (h) Updates the system security and privacy plan whenever significant changes or updates occur;
- (i) Advises the information owner regarding security considerations in applications systems procurement or development, implementation, operation and maintenance, and disposal activities (e.g., life cycle management);
- (j) Participates in risk assessments and audits regarding the system's safeguards; and

- (k) Reports and responds to information security incidents in accordance with the Incident Response Policy.

Supplemental Guidance: The role of the information system owner can be interpreted in a variety of ways depending on the particular agency and the system development life cycle phase of the information system. Some agencies may also refer to information system owners as program managers or business/asset/mission owners.

## **OR-16: INFORMATION OWNER**

The information owner is the agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. The information owner has the following responsibilities related to systems security:

- (a) Assigns the security categorization, ensuring the protection standard, and establishing the rules for the appropriate use of the information;
- (b) Ensures the collection and handling of information is compliant with all applicable laws, regulatory, and contractual requirements, and policies;
- (c) Ensures the collection of personal information is limited to that which is needed for legitimate business purposes and in accordance with all statutory, regulatory, contractual, and policy requirements, and is retained only as long as necessary;
- (d) In concert with the privacy officer, provides proper notice of the collection of personal information in accordance with all statutory, regulatory, contractual, and policy requirements;
- (e) Assists in the identification and assessment of the common security controls where the information resides;
- (f) Provides input to information system owners regarding the security requirements and security controls for the information system(s) where the information is generated, stored, processed, or transmitted;
- (g) Defines precautions for controlling access to, and preserving the security and integrity of, information assets that have been categorized as requiring such precautions;
- (h) Authorizes access to the information in accordance with the security categorization of the information, and the legitimate business need for access to the information; and
- (i) Participates in risk assessments and audits regarding the system's safeguards.

Supplemental Guidance: The role of the information owner in the context of security differs from that of the data owner in the context of the data governance model.

## **OR-17: ASSET CUSTODIAN**

Under the direction of the information system owner and the information owner, asset custodians are responsible for the technical implementation and management of information

assets. Asset custodians have responsibility for the day-to-day operational-level functions on behalf of the information system owner and the information owner. Typically, asset custodians will include systems administrators, network administrators, database administrators, or other designated information technology personnel.

Asset custodians are responsible for ensuring that the assets are properly secured, maintained, are used for the purposes intended, and that information regarding the equipment is properly documented. The asset custodian is responsible for receipt, transfer, accounting, safeguarding, and destruction of an information asset (e.g. information system) commensurate with the information's security categorization. Asset custodians have the following responsibilities related to information security:

- (a) Assists in the development of the System Security and Privacy Plans and contingency plans for all information systems under their purview;
- (b) Implements technical security controls in accordance with the System Security and Privacy Plan and all applicable statutory, regulatory, contractual and policy requirements;
- (c) Complies with any additional security requirements established by the Information System Owner, the Information Owner and/or the Agency CISO;
- (d) Develops and maintains documentation regarding the design, implementation, operation, and security of the information system;
- (e) Maintains and updates the inventory of the components (servers, network hardware, software, operating systems, patch levels, etc.) that comprise the information system;
- (f) Advises the Information System Owner, the Information Owner and the Agency CISO of vulnerabilities that may present a threat to the confidentiality, integrity, availability, and privacy of the information system and/or the information;
- (g) Monitors the security of the information system and reports and responds to security incidents in accordance with the Incident Response Policy;
- (h) Notifies the Information System Owner, Information Owner, and the Agency CISO of any actual or attempted violations of security policies, practices, and procedures;
- (i) Participates in certification and accreditation process for the system, as well as, risk assessments and audits regarding the system's safeguards; and
- (j) Abides by all information security policies and standards.

## **OR-18: AGENCY HUMAN RESOURCES (HR) PERSONNEL**

Agency Human Resources personnel shall fulfill the following responsibilities in support information security program:

- (a) Assists in the development, distribution, communications, and enforcement of the Statewide Information Security Manual's Policies and Standards;
- (b) Coordinates and administers the employee screening and background check process;

- (c) Notifies the Agency CIO or his/her designee of new employees' security access privileges according to their role and responsibilities;
- (d) Notifies the Agency CIO or his/her designee of updates to employees' security access privileges according to changes in employment status, including promotions, transfers, and terminations;
- (e) Administers the new employee orientation program which includes the requirement to complete the Information Security Awareness and Training within thirty (30) days of hire;
- (f) In coordination with the Agency CISO assists with the administration and tracking of compliance with the Security Awareness and Training requirements;
- (g) Assists in the investigation and handling of information security policy violations, as appropriate; and
- (h) Reports information security incidents in accordance with the Incident Response Policy, and the respective agency incident response plan.

## **OR-19: OFFICE OF THE ATTORNEY GENERAL PERSONNEL**

The Office of the Attorney General personnel shall fulfill the following responsibilities in support of the information security program:

- (a) Protects the State's intellectual property rights;
- (b) Provides advice and counsel regarding policies and standards, legislation, regulations and contractual terms;
- (c) Provides advice, counsel, and investigative support regarding information security incidents;
- (d) Acts as the primary point of contact for external legal services related to information security incidents;
- (e) Assists in the development and evolution of the Executive Branch of New Jersey State Government's Statewide Information Security Manual to ensure currency with legislative and regulatory changes and obligations;
- (f) Reviews contracts and agreements to ensure that information security-related issues are addressed;
- (g) Assists with the development and execution of privacy and security agreements for services provided by third-party vendors; and
- (h) Assists with the development and execution of information sharing agreements.

## **OR-20: USER**

All Executive Branch agency full-time and part-time employees, temporary workers, volunteers, interns, contractors, and those employed by contracted entities, collectively referred to as users, are individuals authorized to access, and have a need to use, State information assets as part of

their assigned duties or in fulfillment of assigned roles or functions. Users are considered both custodians of the information assets and information they are provided for use in the performance of their duties and are required to uphold all applicable information security policies and standards.

- (a) Users are responsible for protecting information assets against their accidental or unauthorized disclosure, modification, and destruction, and for assuring the confidentiality, integrity, availability, and privacy of information and information assets;
- (b) Individuals acting in a supervisory or management capacity are responsible for information security within their respective supervisory area. This responsibility includes supporting and ensuring compliance with the Statewide Information Security Manual's policies and standards; and
- (c) All users are responsible for understanding and complying with requirements of the Statewide Information Security Manual's policies and standards.

## **OR-21: SEPARATION OF DUTIES**

Agencies shall implement a separation of duties for all roles and operations that can impact the security of their information assets including, but not limited to, the following:

- (a) Individuals fulfilling governance, compliance, and auditing roles should be independent from the functions they audit;
- (b) The separation of security administration through which individuals and groups are provided access to information assets and those who act in other capacities, including, but not limited to, systems administration, application development, database management, etc., should be implemented to the fullest extent practical to meet business and security objectives;
- (c) Application development personnel should not have access to production data or systems-level technology;
- (d) Systems administrators should not have access to application code that would allow for them to make changes to the code;
- (e) Database administrator access should be sufficiently restricted such that they can perform administrative functions without the option to retrieve sensitive information;
- (f) Administrative access to firewalls, routers, switches, and other networking equipment and systems should be limited to authorized networking personnel; and
- (g) Administrative access to information security systems and technologies should be limited to authorized personnel.

Supplemental Guidance: It is important to identify key IT personnel to minimize reliance on a single individual performing a critical job function through knowledge capture (documentation), knowledge sharing, succession planning and staff backup.

## **OR-22: CONTACTS WITH EXTERNAL ORGANIZATIONS**

The NJOHSP New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) shall develop and maintain relationships with external organizations to stay abreast of current and emerging security issues. Additionally, the NJCCIC shall maintain appropriate contacts with external organizations and entities to ensure that appropriate actions can be quickly taken, and advice obtained, in the event of a security incident. These contacts should include, but are not limited to, the following:

- (a) Law enforcement authorities;
- (b) Regulatory agencies;
- (c) Incident response management service providers;
- (d) Information security professional organizations;
- (e) Information technology and telecommunications service providers; and
- (f) Others, as necessary, to protect the Executive Branch of State Government information assets.

## **OR-23: INDEPENDENT REVIEW OF INFORMATION SECURITY PROGRAM**

The State Chief Information Security Officer shall periodically engage external assessors and auditors to conduct independent reviews of the Executive Branch of State Government information security program. In addition, the State CISO, in coordination with State agencies, will engage independent external assessors to ensure accreditation and certification of its information security program as it relates to the State's statutory, regulatory, and contractual obligations.

## **OR-24: REPORTING OF INCIDENTS**

All personnel are required to immediately report any suspected information security incident. Suspected information security incidents may be reported via the following channels:

- Immediate supervisor;
- Agency HR Representative;
- Agency IT Service Desk;
- Agency Information Security Office;
- NJOIT Enterprise Service Desk – 1.800.622.4357; or
- NJ Cybersecurity and Communications Integration Cell – 833.465.2242 (1.833.4.NJCCIC) or <https://www.cyber.nj.gov/cyber-incident/>

Any attempt to interfere with, prevent, obstruct, or dissuade a user in their efforts to report a suspected security incident or violation is strictly prohibited and cause for disciplinary action, up to, and including, termination. Any form of retaliation against an individual reporting or investigating a security incident or violation is also prohibited.

## **REFERENCES**

The requirements established in the Organizational Security Policy have been derived from the following:

NIST SP 800-53r5 Program Management (PM), Personnel Security (PS); and  
NIST CSF Identify/Governance (ID.GV).

---

## PERSONNEL SECURITY (PS)

---

### PS-01: PURPOSE

The purpose of the Personnel Security policies and standards is to ensure that all Executive Branch of New Jersey State Government personnel have the appropriate background, skills, and training to perform their job responsibilities in a competent, professional, and secure manner.

### KEY TERMS

**Access** - Ability to make use of any information system or resource.

**User** – The term “user” refers to any Executive Branch agency full-time or part-time employee, temporary worker, volunteer, intern, contractor, and those employed by contracted entities who are provided authorized access to State information assets.

**Sensitive Information** - A term used to describe any information which requires protection from unauthorized access or disclosure.

**Information Asset** - A term used to describe any data, device, or other component of an information or communications system. Assets generally include hardware (e.g. servers, laptop and desktop computers, switches), software (e.g. commercial off the shelf and custom developed applications and support systems), cloud services, and information. Assets may also be referred to as information systems or resources.

### PS-02: POLICY

Agencies shall implement personnel security procedures to ensure that individuals with authorized access to agency information assets have the requisite skills and training to carry out their job functions. All full-time and part-time employees, temporary workers, volunteers, interns, contractors, and those employed by contracted entities shall have the appropriate background, skills, and training to perform their job responsibilities in a competent, professional, and secure manner.

Agencies shall establish workforce security procedures that meet, or exceed, the minimum information security controls as listed below.

### PS-03: POSITION RISK DESIGNATION

Agencies shall assign risk designations to all position descriptions within their agency.

Supplemental Guidance: Position risk designations provide guidance for the risk associated to a given role. Examples of high-risk designations include individuals with access to highly sensitive information assets and individuals that hold master keys or access to data centers or other sensitive/critical facilities. Risk designations provide guidance on the level of personnel screening, security clearances, and training for a given role. Agency management should work with their

respective human resources representatives and security personnel to identify security concerns associated with position responsibilities.

## **PS-04: PERSONNEL SCREENING**

Prior to authorizing access to agency information assets, agencies shall conduct personnel screening checks in accordance with applicable state and federal laws for all full- and part-time employees, contractors, consultants, interns, volunteers, and business partners.

- (a) The level of background verification checks shall be commensurate with the role, responsibilities, level of access to be granted, and the risk designation assigned to the position;
- (b) Agencies shall include personnel screening requirements in all contracts with consultants, contractors, and vendors that are to be provided with access to agency information assets; and
- (c) Supplemental employment screening may be conducted for individuals who are in key positions or with privileged access to agency information assets.

Supplemental Guidance: Criminal background checks may be required by state or federal law based on role and/or access to sensitive information. Information types for which access requires the successful completion of a criminal background check includes, but is not limited to, Federal Tax Information (FTI), Criminal Justice Information (CJI), and Centers for Medicaid and Medicare System (CMMS) information.

Agencies should review the information they generate, process, store, and transmit to determine applicable laws governing access and background check requirements.

## **PS-05: TRANSFERS AND PROMOTIONS**

Agencies shall ensure that a review of security access and job responsibilities are performed by the releasing and receiving managers when an employee is promoted, transferred to another Department, Agency, or organization unit, or takes on a different role, to ensure appropriate access levels to information assets.

If an employee is given added responsibility at a key position through transfer or promotion, an additional background check and screening should be considered if permitted and/or required by applicable laws and regulations.

## **PS-06: PERSONNEL TERMINATION**

Agencies are required to ensure that upon termination of an individual's employment or contract the following procedures are executed:

- (a) Upon notification of termination, immediately disable access to State information systems;
- (b) Terminate/revoke any authenticators/credentials associated with the individual;

- (c) Retrieve all State property (e.g., keys, identification badges, proprietary and confidential information, laptops, tablets, phones, storage media, and hardware authentication tokens);
- (d) Conduct exit interviews to ensure that the terminated individual understands the security constraints imposed by being a former employee and that proper accountability is achieved for information system-related property; and
- (e) For continuity of business purposes, ensure that appropriate agency personnel retain access to departing employee's information stores (e.g. email and local and network data).

Supplemental Guidance: Timely execution of termination action is essential for individuals terminated for cause. In certain situations, agencies should consider disabling the information system accounts of individuals that are being terminated prior to the individuals being notified.

Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and unavailability of supervisors.

## **PS-07: ACCESS AGREEMENTS**

Agency management shall:

- (a) Develop and document access agreements for agency information systems;
- (b) Annually review and update the access agreements if appropriate; and
- (c) Ensure that individuals requiring access to agency information and information systems review and acknowledge access agreements prior to being granted access, and at least annually thereafter.

Supplemental Guidance: Access agreements include, for example, non-disclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with agency information systems to which access is authorized. Agencies can use electronic signatures to acknowledge access agreements unless specifically prohibited by agency policy.

## **PS-08: THIRD-PARTY PERSONNEL SECURITY**

Agencies shall:

- (a) Establish personnel security requirements, including security roles and responsibilities, for third-party providers that must, at a minimum, comply with the Rules of Behavior/Acceptable Use requirements included in this Manual and those established by the contracting agency;
- (b) Require third-party providers to comply with personnel security policies and procedures established by the agencies;

- (c) Document and ensure third-party providers acknowledge the personnel security requirements;
- (d) Require third-party providers to notify the designated agency liaison of any personnel transfers or terminations of third-party personnel who possess agency credentials and/or badges, or who have information system privileges within the agency; and
- (e) Monitor the third-party provider for compliance with rules of behavior and acceptable use policies.

Supplemental Guidance: Third-party providers include, for example, service bureaus, contractors, and other organizations or companies providing information system development, information technology services, outsourced applications, and network and security management.

## **PS-09: RULES OF BEHAVIOR**

The use of State information assets is permitted for authorized State government business purposes to support the goals and objectives of the Executive Branch of New Jersey State Government departments and agencies. Accordingly, State information assets are to be used in a manner that is consistent with applicable laws and regulations, in accordance with all New Jersey State Government policies, and as part of the individual's assigned duties and responsibilities.

## **PS-10: AGENCY REQUIREMENTS**

Agency management shall:

- (a) Develop rules of behavior and acceptable use requirements that, at a minimum, incorporate the listed user requirements detailed below.
- (b) Ensure that users acknowledge in writing or electronically their understanding of, and agreement to abide by, the terms set forth in the agency's acceptable use policy.
- (c) Ensure users are provided with security awareness training in accordance with the Security Awareness and Training Policy. Users are to be made aware of the security risks associated with their roles and understand their responsibilities, as well as applicable laws, policies, standards, and procedures related to the security of State information assets.

## **PS-11: USER REQUIREMENTS**

The rules of behavior and requirements contained in this Manual apply to all users of State information assets, regardless of the agency, role, or location. All uses of State information assets must comply with State of New Jersey policies, standards, procedures, and guidelines, as well as all applicable Federal and State laws. Certain users, subject to approval from agency management, may be exempted from certain requirements during the course of their legitimate job responsibilities. The following list of user requirements is by no means

exhaustive, but attempts to provide a framework for activities that fall into the categories of generally acceptable and unacceptable use.

- (a) Users are responsible for protecting State information and resources from unauthorized use or disclosure;
- (b) Individuals who are provided with portable information assets including, but not limited to: laptop computers, tablets, smart phones, removable media, etc., shall be responsible for the physical security and condition of these information assets;
- (c) Users shall immediately report lost or stolen State information assets, suspected policy violations, suspected information security incidents, and suspicious activity in accordance with their agency's reporting procedures;
- (d) User are prohibited from performing any act that is illegal or otherwise in violation of any applicable federal or state laws, or State policies;
- (e) Users are prohibited from accessing State information and/or systems without express authorization;
- (f) Users are prohibited from sharing account passwords, Personal Identification Numbers (PINs), security questions/answers, security tokens (e.g., smartcard, key fob), or similar information or devices used for authentication and authorization to State information assets;
- (g) Users are prohibited from engaging in the subversion of existing security controls (e.g. network, computer, or device hacking and scanning, password cracking, penetration testing, and conducting red team exercises, etc.) unless expressly authorized by the State Chief Information Security Officer or his/her designee;
- (h) Users are prohibited from purposely introducing malicious programs (e.g., malware, viruses, worms, trojan horses, etc.) into the network or server ;
- (i) Users are prohibited from accessing, transmitting, storing, or creating any discriminatory, defamatory, offensive, disruptive or otherwise inappropriate content including, but not limited to: websites that contain sexually suggestive images or content, racial slurs, gender specific comments, or any other comments that inappropriately or unprofessionally address someone's age, race, gender, color, national origin, religion, sexual orientation, disability, or veteran status;
- (j) Users are prohibited from creating, sending, and forwarding unsolicited email messages, including the sending of junk mail, chain letters, Ponzi or pyramid schemes, or other advertising material (email spam) to individuals who did not specifically request such material;
- (k) Users are prohibited from sending email under another individual's name or email address, except when authorized to do so by the owner of the email account for a work-related purpose;
- (l) Users are prohibited from installing, downloading, or running software that has not been approved by agency management;

- (m) Users are prohibited from adding or installing personal IT resources (e.g. wireless access points, software, mobile devices, etc.) to existing State information systems without the appropriate management authorization;
- (n) Users are prohibited from establishing new Internet web and/or social media pages, accounts, or content dealing with State business, or making modifications to existing pages, accounts, or content dealing with State business without express authorization by agency management;
- (o) Users are prohibited from transmitting, storing, processing, or sharing sensitive State information using personal or other unauthorized Internet services, including but not limited to: personal email accounts, social media accounts, chat services, file storage, file synchronization, file sharing, and other unauthorized services;
- (p) Users are prohibited from sharing sensitive information without authorization;
- (q) Users are prohibited from purposely acquiring, using, reproducing, transmitting, or distributing any information, software or other electronic materials (e.g. movies, music) in violation of applicable copyright, trademark, intellectual property laws, and contractual agreements;
- (r) Users are prohibited from using State information assets to conduct or promote user's outside employment or business interests;
- (s) Users are prohibited from using State information assets to conduct political activity, such as lobbying elected officials and participating in partisan political activities, without authorized approval; and
- (t) Users are prohibited from using State information assets to circulate unauthorized solicitations or advertisements for non-State purposes including religious, political, or not-for-profit entities.

## **PS-12: INCIDENTAL USE OF STATE OF NEW JERSEY INFORMATION ASSETS**

State of New Jersey information assets are provided for the purpose of conducting State business. Incidental use of State information assets for personal purposes is permitted when such use does not interfere with the user's performance, does not expose the State to unnecessary risks, does not result in additional cost to State agencies, and does not violate any policies, applicable laws, regulatory, contractual requirements, or existing labor agreements.

Agencies and users' managers may adopt more restrictive incidental use policies.

## **PS-13: REPORTING OF INCIDENTS**

Agencies shall develop procedures to ensure all personnel are aware of their duty to protect State information assets and their responsibility to immediately report any suspected information security incident. Suspected information security incidents may be reported via the following channels:

- Immediate supervisor;
- Agency HR Representative;
- Agency IT Service Desk;
- Agency ISO;
- NJOIT Network Control Center – 1.800.622.4357; or
- NJ Cybersecurity and Communications Integration Cell – 1.833.465.2242 (1.833.4.NJCCIC) or <https://www.cyber.nj.gov/cyber-incident/>.

Any attempt to interfere with, prevent, obstruct, or dissuade a user in their efforts to report a suspected security incident or violation is strictly prohibited and cause for disciplinary action, up to and including termination. Any form of retaliation against an individual reporting or investigating a security incident or violation is also prohibited.

## **PS-14: NO EXPECTATION OF PRIVACY**

Information assets purchased, leased, or licensed by the State of New Jersey including, but not limited to: software (e.g. application software, application source code, systems software), physical equipment (e.g. computers, portable devices, tablets, smartphones), communications equipment (e.g. routers, switches, firewalls), electronic media (e.g. disks, tapes), services (e.g. Internet, communications, cloud), and information (e.g. databases and data files, system documentation, network diagrams) are the property of the State of New Jersey. As such, the State has the absolute right to monitor the use of such property. Accordingly, users of State information assets shall not assume their actions or use of State information assets are private or protected.

## **PS-15: SECURITY MONITORING**

In order to protect State information assets against security threats and to ensure compliance with the State and agency-specific policies, as well as applicable contractual, regulatory, and statutory requirements, State agencies have the right to implement security monitoring technologies and systems including, but not limited to: anti-virus/anti-malware software, firewalls, host and network intrusion protection and intrusion detection systems, vulnerability management systems, database and application monitoring systems, data loss prevention, and web and email content filtering systems. As permissible by law, the agencies' security monitoring systems and their authorized personnel have the right to monitor, audit, review, block, and log any traffic sent or received by users of State information assets, and any network traffic emanating from or sent to agency networks, systems, applications, databases or other information assets, as well as any traffic directed at the State's information assets from external sources.

## **PS-16: PERSONNEL SANCTIONS**

Compliance with the above Personnel Security requirements is a requirement of employment or contract. Users who are found in violation of the requirements are subject to disciplinary action

up to and including termination of employment, or immediate termination of contractor and/or vendor relationship. Violations of law may be referred to the appropriate law enforcement agency for investigation and prosecution.

## REFERENCES

The requirements established in the Personnel Security policies and standards have been derived from the following:

- NIST SP 800-53r5 Personnel Security (PS), Planning (PL); Access Control (AC); Security Assessment and Authorization (CA);
- NIST CSF Protect/Information Protection Processes and Procedures (PR.IP);
- [FBI Criminal Justice Information Security Policy](#);
- IRS Publication 1075 - [Safeguards for Protecting Federal Tax Returns and Return Information](#);
- Centers for Medicare & Medicaid Services, [Minimum Acceptable Risk Standards for Exchanges, version 2.0 \(MARS-E\)](#);
- [State of New Jersey Civil Service Commission Policies and Procedures](#);
- [New Jersey Conflicts of Interest Law](#); and
- [Plain Language Guide to New Jersey's Executive Branch Ethics Standards](#).

---

## SECURITY AWARENESS AND TRAINING (AT)

---

### AT-01: PURPOSE

The purpose of the Security Awareness and Training policies and standards is to ensure users are aware of information security and privacy risks and threats to State information assets, understand their responsibilities, and are aware of the statutory and policy requirements that are intended to protect State information and information systems from a loss of confidentiality, integrity, or availability.

### KEY TERMS

**Computer-Based Training (CBT)** - Any course of instruction whose primary means of delivery is a computer. A CBT course (sometimes called courseware) may be delivered via a software product installed on a single computer, through an agency or the State intranet, or over the Internet as web-based training.

### AT-02: POLICY

Agency management shall ensure that all users are made aware of the security and privacy risks associated with their roles and that users understand their responsibilities, as well as applicable laws, regulations, executive orders, circulars, policies, standards, and procedures related to the security and privacy of State information and systems.

### AT-03: INFORMATION SECURITY AND PRIVACY AWARENESS PROGRAM

The State Chief Information Security Officer (CISO) is responsible for developing and implementing an enterprise information security and privacy awareness program that is to be administered to all full and part-time employees, interns, volunteers, contractors, and those employed by contracted entities, by their respective agencies.

- (a) The information security awareness and training program shall be developed to make State personnel aware of the importance of information security and privacy, as well as to provide them with an understanding of State information security and privacy policies, laws, and regulations that govern their use of State information systems and information.
- (b) The NJCCIC licenses an online computer-based training (CBT) information security and privacy awareness program that all Executive Branch agencies are to use to provide agency personnel with a basic literacy of information security and privacy concepts and an understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents.
- (c) Agencies are required to develop and implement security awareness training that supplements the content of enterprise program with content that addresses the risks,

applicable laws and regulations, and responsibilities for users within their respective agencies.

Supplemental Guidance: Agency management should contact the NJCCIC at [cybertraining@cyber.nj.gov](mailto:cybertraining@cyber.nj.gov) to request access to the NJCCIC-licensed CBT program. NJCCIC-licensed CBT modules cover the following security-related topics:

- Social Engineering
- Phishing
- Insider Threat
- Email and Phishing
- Browsing Safety
- Working Remotely
- Passwords
- Physical Security
- International Travel
- Personally Identifiable Information (PII)
- Federal Tax Information (FTI)
- Health Insurance Portability and Privacy Act (HIPAA)
- Data Security
- Encryption
- Social Media
- Mobile Devices
- Targeted Attacks
- Privileged Access
- Cloud Security
- Ethics
- Creating a Cyber Secure Home
- Protecting Children Online
- Privacy
- General Data Protection Regulation (GDPR)

In addition to CBT training, the NJCCIC publishes a monthly Employee Security Awareness Bulletin that is delivered to all State employees. State employees are encouraged to subscribe to other NJCCIC publications that cover relevant security alerts, advisories, and best practices. Additional security and privacy information may also be accessed from the NJCCIC website at [cyber.nj.gov](http://cyber.nj.gov). Agencies should provide training on agency policies, acceptable use of State information assets, incident reporting responsibilities, etc.

#### **AT-04: INFORMATION SECURITY AND PRIVACY TRAINING**

- (a) Agency management are responsible for ensuring that all new personnel complete security and privacy awareness training within thirty (30) business days of their start of employment as part of the required new hire training curriculum; and
- (b) Agency management shall ensure that all users who have authorized access to State information systems complete security awareness and privacy training at least annually, to ensure that they are aware of their responsibilities with regard to information security and privacy.

Supplemental Guidance: Training should focus on ensuring users have a basic understanding of the need for information security and user actions to maintain security and to respond to suspected incidents.

## **AT-05: ROLE-BASED SECURITY AND PRIVACY TRAINING**

Agencies shall:

- (a) Provide role-based security and privacy training that addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical controls. Role-based training also includes policies, procedures, tools, methods, and artifacts for the security and privacy roles defined. Agencies shall provide role-based training:
  1. Before authorizing access to the system, information, or performing assigned duties, and at least annually thereafter; and
  2. When required by system or organizational changes;
- (b) Periodically update role-based training content; and
- (c) Incorporate lessons learned from internal or external security incidents or breaches into role-based training.

Supplemental Guidance: Agencies are advised to determine the content of training based on the assigned roles and responsibilities of individuals as well as the security and privacy requirements of the agency and the systems to which personnel have authorized access, including technical training specifically tailored for assigned duties.

## **AT-06: PRACTICAL EXERCISES**

The NJCCIC shall:

- (a) Provide practical exercises across Executive Branch agencies that simulate events and incidents; and
- (b) Provide role-based practical exercises in security and privacy training that reinforce training objectives.

Supplemental Guidance: Practical exercises include no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links. Practical exercises for role-based security include training for software developers that addresses simulated attacks that exploit common software vulnerabilities or spear or whale phishing attacks targeted at senior leaders or executives. Practical exercises for privacy include modules with quizzes on identifying and processing personally identifiable information in various scenarios or scenarios on conducting privacy impact assessments.

## **AT-07: TRAINING RECORDS**

Agencies shall:

- (a) Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and
- (b) Retain individual training records in accordance with State and agency-specific records retention requirements.

Supplemental Guidance: The New Jersey Civil Service Commission manages and administers the State's Learning Management System (LMS) that automatically records completion of the required CBT training provided by the NJCCIC.

## **AT-08: SECURITY ADVISORIES AND ALERTS**

The New Jersey Cybersecurity Communications and Integration Cell shall provide State agencies with current and relevant security-related advisories and alerts on a periodic basis. Such alerts and advisories may be distributed via email, phone, text message, Internet or Intranet postings, or other communications medium, as appropriate.

## **AT-09: INFORMATION SECURITY RESOURCES**

The NJCCCIC shall create, post, maintain, and make available to all agencies any information security policy documentation, training materials, security guidelines, advisories, alerts, etc.

## **REFERENCES**

The requirements established in the Security Awareness and Training policies and standards have been derived from the following:

- NIST SP 800-53r5 Awareness Training (AT), Program Management (PM); and
- NIST CSF Protect/Awareness and Training (PR-AT).

---

## RISK ASSESSMENT (RA)

---

### RA-01: PURPOSE

The purpose of the Risk Assessment policies and standards is to establish requirements for the identification, assessment, treatment, and monitoring of information security and privacy risks to agency operations, information systems, and information.

### KEY TERMS

**Business Critical** - Includes systems, services, and data that are important to the support of an agency's business operations.

**Criticality** - A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function.

**General Support System** - a general support system is an interconnected set of information resources under the same direct management control that shares common functionality. A general support system normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. A general support system, for example, can be a:

- (a) Local area network (including workstations, printers, and other assets that support an agency office or facility);
- (b) Backbone network (e.g. agency-wide and/or statewide (GSN));
- (c) Agency data processing center including its operating system and utilities (e.g. server room); and/or
- (d) Shared information processing service facility (e.g. data center).

**Major Applications and Systems** - A major application or system is defined as any system or application that includes one or more of the following characteristics:

- (a) Includes users in more than one agency;
- (b) Costs more than \$200,000 to develop and implement (cost includes hardware, software, and contract personnel);
- (c) Any public facing web application; and/or
- (d) Any application that stores or processes sensitive information or is deemed critical to the operations of the agency.

**Minor Applications and Systems** – consist of those systems and applications not considered major applications or general support systems. Often times minor applications are components of a major application or system.

**Mission Critical** - Includes systems, services, and data that are determined to be vital to the operations or mission effectiveness of an agency or multiple agencies. Availability of this information must be rigorously protected.

**Non-Critical** - Includes systems, services, and data that are necessary for day-to-day operations, but are not critical to an agency's mission or core functions.

**Non-Sensitive Personally Identifiable Information (PII)** - Information that is available in public sources the disclosure of which cannot reasonably be expected to result in personal harm.

**Risk** - The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

**Risk Assessment** - The process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation, arising through the operation of an information system. Part of risk management and synonymous with risk analysis, risk assessment incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place.

**Risk Management** - The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, the State, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.

**Risk Mitigation** - Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

**Threat** - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

**Vulnerability** - Weakness in information systems, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

## **RA-02: RISK ASSESSMENT POLICY**

Agencies shall implement continuous risk management processes that account for the identification, assessment, treatment, and monitoring of risks that can adversely impact their operations, information systems, and information.

## **RA-03: SECURITY CATEGORIZATION**

Asset owners, in conjunction with asset custodians, information security and privacy officers, and other key stakeholders, shall categorize information assets and the information they store,

process, and transmit according the level of impact should there be a loss of confidentiality, integrity, and/or availability of the asset or information.

## **RA-04: DATA CLASSIFICATION**

Agencies shall classify all information generated, collected, stored, processed, or transmitted by State of New Jersey information systems in accordance with all applicable statutory, regulatory, and contractual requirements and according to the information's sensitivity, along with an assessment of risks associated with the potential loss of confidentiality, integrity, availability, or privacy.

The following data classification schema is to be used when classifying data.

**Public:** Information that is intended, or required, to be shared with the public.

**Internal Use:** Non-sensitive information that is used in the daily operations of an Agency.

**Confidential:** Sensitive information that is used or held by an Agency. Considerable loss or harm could occur as a result of unauthorized access, use, or disclosure of this information.

**Restricted:** Highly sensitive information that is used or held by an agency. Statutory or regulatory penalties, notification provisions, or other mandates could result if the information is accessed, used or disclosed in an unauthorized manner.

## **RA-05: DATA CLASSIFICATION AND SECURITY CATEGORIZATION CONSIDERATIONS**

The considerations listed below must be evaluated by agencies when assigning security categorizations to their information assets and determining the impact should a loss of confidentiality, integrity, availability, or privacy be realized.

- (a) **Legal, Regulatory, Contractual, and Policy Compliance** - Various federal and state laws, regulations, contracts and policies mandate the protection of personal information from unauthorized access, use, or disclosure. Questions regarding laws and regulations that apply to specific agencies and the information they collect, store, process, or output should be directed to the agency's legal counsel (Office of the Attorney General).
- (b) **Personal Information** – New Jersey Revised Statutes §56:8-161 (2013) defines Personal Information as an individual's first name or first initial and last name linked with any one or more of the following data elements: (1) Social Security number; (2) driver's license number or State identification card number; or (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.
- (c) **Personally Identifiable Information (PII)** - NIST Special Publication (SP) 800-121 defines PII as any information about an individual maintained by an agency, including

- (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and
- (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Examples of PII include but are not limited to the following:

- Name, such as full name, maiden name, mother's maiden name, or alias Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number;
- Address information, such as street address or email address;
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well defined group of people;
- Telephone numbers, including mobile, business, and personal numbers;
- Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry);
- Information identifying personally owned property, such as vehicle registration number or title number and related information; and
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

(d) **Sensitive Personally Identifiable Information (SPII)** - Personal information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

(e) **Criminal Justice Information** - is the term used to refer to all of the FBI Criminal Justice Information Services provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

- **Biometric Data** - data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.
- **Identity History Data** - textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.

- Biographic Data -information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
- Property Data -information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).
- Case/Incident History - information about the history of criminal incidents.

(f) **Federal Tax Information (FTI)** - FTI consists of federal tax returns and return information (and information derived from it) that is in the agency's possession or control which is covered by the confidentiality protections of the [Internal Revenue Code](#) (IRC) and subject to the IRC 6103(p)(4) safeguarding requirements including IRS oversight. FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to an IRC 6103(p)(2)(B) Agreement.

FTI includes any information created by the recipient that is derived from federal return or return information received from the IRS or obtained through a secondary source.

(g) **Electronic Protected Health Information (ePHI)** – Electronic Protected Health Information (PHI) consists of any information about health status, provision of health care, or payment for health care that can be linked to an individual. PHI refers to all “individually identifiable information” held or transmitted by the State Entities or its business associates in any form or media, whether paper, electronic or oral. “Individually identifiable health information” is information, including demographic data, that relates to:

- The individual's past, present, or future physical or mental health or condition,
- The provision of health care to the individual, or
- The past, present, or future payment for the provision of health care to the individual,
- The individual's identity or for which there is a reasonable basis to believe it can be used to identify the individual.

(h) **Social Security Administration Provided Information** – is information that is obtained from the Social Security Administration (SSA). This can include a Social Security number verification indicator or other PII data.

(i) **Payment Card Industry (PCI) Data Security Standard (DSS) Information** – PCI DSS applies to the transmission, storage, or processing of confidential credit card data. This data classification includes credit card magnetic stripe data, card verification values, payment account numbers, personally identification numbers, passwords, and card expiration dates.

(j) **Potential Harm to Individuals** - Agencies must consider any potential harm or adverse impact that the compromise of information may have on the parties to whom the information pertains.

- (k) **Agency Mission and Business Objectives** - Agencies must consider their mission and business objectives when assigning information classifications. Certain agencies may be obligated to share as much of their data as possible with the public or other outside agencies while others may be under the strictest constraints in ensuring that their data is protected against any exposure whatsoever. In either case, while it is incumbent on the agency to ensure that those objectives are met, adequate controls need to be in place and in effect to address confidentiality, integrity, availability, and privacy.
- (l) **Information System Dependencies/Connections and Aggregation/Commingling of Information** - Agencies must consider the risks associated with information system dependencies and connections to other systems when classifying information. Low-sensitivity information protected by the minimum required controls in isolation must implement more restrictive controls when connected to systems containing high-sensitivity information. Information owners must consider the sensitivity of information types in the aggregate when assigning classifications. The confidentiality of an individual's first and last name is not considered High Impact information on an isolated system. When connected to, combined with, or commingled on, a system that includes other identifiers such as a social security number, the aggregate of the information requires classification as High Impact, highly sensitive and requires appropriate controls necessary to ensure the confidentiality of the information is maintained.
- (m) **Information Sharing Agreements, Memorandums of Understanding, and Contractual Requirements** - Information Sharing Agreements, Memoranda of Understanding (MOU), grants, contracts, and other written agreements between agencies and external entities may include agreements regarding information access, sharing, use, disclosure and maintenance of information, as determined by the information classification of the information owner. The recipient organization's information risk classification must align with any such requirements. Additionally, if an agreement states that the recipient agency may further share the information, the subsequent recipients must adhere to the requirements of the original classification.
- (n) **Intellectual Property** - Agencies must consider any intellectual property rights owned by an entity other than the State agency, when determining information risk classification assignments.
- (o) **Information Lifecycle** - Agencies must consider the risk classification of information throughout its lifecycle as changes may occur prompting changes to the classification and the associated security controls. As an example, contract bids prior to award are classified as High Impact information. Post award, the risk classification of contract bids may be lowered and thus require less protective controls regarding confidentiality.
- (p) **Metadata** - Agencies must consider metadata when classifying information. Metadata is often referred to as "data about data". Metadata describes or supplements the information and may be either separate from or embedded within documents, records, or objects. Examples of metadata include filename, creation date, file size, author, etc. While metadata

may not be readily readable, the sensitivity of the metadata alone or in combination with the information, needs to be considered.

Supplemental Guidance: Agencies should consult with agency security and privacy officers and legal counsel when determining data classifications. A non-exhaustive list of examples of commonly held data and their classifications are included in the table.

<b>RESTRICTED</b>	<b>CONFIDENTIAL</b>	<b>INTERNAL USE</b>	<b>PUBLIC</b>
Federal tax information received from, or derived from, the IRS or secondary sources (IRS Pub. 1075)	Pension/Retirement benefit information (actual amounts)	Agency policies, procedures, and/or standards	Public-facing website content
Protected Health Information (HIPAA/HITECH)	Personal demographics (race, place of birth, weight, religion)	Training materials	Publicly distributed information
Social Security numbers	Unpublished information about Agency personnel such as home telephone numbers and home addresses used for emergency contact	Internal meeting information	Meeting agendas and minutes from public meetings
Debit or credit card numbers		Direct telephone line numbers to staff	Brochures Press releases
Driver's license information or State identification card Information	All information exempt from disclosure pursuant to New Jersey Open Public Records Act, N.J.S.A. 47:1A- 1 et seq		Agency contact information
Bank account numbers or information with personal identification numbers (PINs) or passwords	Information received from and/or about a business (tax information, business plans)		
Passport numbers			
Biometric Identifiers	Security plans, network architecture, etc.		
Child welfare and legal information about minors			

## RA-06: ASSIGNING SECURITY CATEGORIZATIONS

Agencies shall assign security categorizations that represent the impact level should an information system or asset suffer a loss of confidentiality, integrity, or availability. The impact level is a function of the sensitivity and criticality of the system or asset.

(a) Agencies shall use the following impact levels when assigning security categorizations.

**Low:** The loss of confidentiality, integrity, or availability that could be expected to have a limited adverse effect on agency operations, agency assets, individuals, other organizations, or the State of New Jersey, such as:

1. Causes a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
2. Results in minor damage to agency assets;
3. Results in minor financial loss; or
4. Results in minor harm to individuals.

**Moderate:** The loss of confidentiality, integrity, or availability that could be expected to have a serious adverse effect on agency operations, agency assets, individuals, other organizations, or the State of New Jersey, such as:

1. Causes a significant degradation in mission capability to an extent and duration that the agency can perform its primary functions, but the effectiveness of the functions is significantly reduced;
2. Results in significant damage to agency assets;
3. Results in significant financial loss; or
4. Results in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.

**High:** The loss of confidentiality, integrity, or availability that could be expected to have a severe or catastrophic adverse effect on agency operations, agency assets, individuals, other organizations, or the State of New Jersey, such as:

1. Causes a severe degradation in mission capability to an extent and duration that the agency can perform its primary functions, but the effectiveness of the functions is significantly reduced;
2. Results in major damage to organizational assets;
3. Results in major financial loss; or
4. Results in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

(b) Systems shall inherit the categorizations of the information which they generate, store, process, or transmit, and are to be protected accordingly; and

- (c) If more than one categorization could apply to a system or asset, the highest level (most restrictive) shall be applied.

Supplemental Guidance: The following Security Categorization Matrix Guide can be used to assist agencies in determining the security categorizations of their information assets.

SECURITY CATEGORIZATION MATRIX GUIDE		SENSITIVITY			
		RESTRICTED	CONFIDENTIAL	INTERNAL USE	PUBLIC
CRITICALITY/ AVAILABILITY	MISSION CRITICAL	HIGH	HIGH	HIGH	HIGH
	BUSINESS CRITICAL	HIGH	HIGH	MODERATE	MODERATE
	NON-CRITICAL	HIGH	MODERATE	LOW	LOW

When assigning security categorizations to information assets, agencies should document the categorization results, including supporting rationale for the categorization. Agencies must ensure all assets, within an authorization boundary to which a given asset is connected, have required controls applied in accordance with its security categorization.

Security categorization processes carried out by agencies facilitate the development of inventories of information assets and mappings to specific information system components where information is processed, stored, or transmitted. Security categorizations are key elements and should be included in service level agreements and other contract vehicles with service providers.

### RA-07: RISK ASSESSMENTS

Risk assessments shall be conducted throughout the lifecycle of major systems and applications and general support systems to identify, quantify, and prioritize risks against operational and control objectives and to design, implement, and exercise controls that provide reasonable assurance that security objectives will be met, and that risk will be mitigated and managed to an acceptable level. Risk assessments are to be conducted:

- (a) Prior to production implementation of new major systems and applications or general support systems;
- (b) When substantive changes have occurred in major systems or applications, or general support systems;
- (c) After a breach of a system’s information security controls;

- (d) When substantive changes have occurred in the agency information technology or organizational environments; and
- (e) At least annually, based on the criticality of the system and the sensitivity of the information.

Supplemental Guidance: Risk assessments are an ongoing process for all systems. Recurring assessments should be prioritized based on the information system's criticality and the sensitivity of the information the system processes, stores, and transmits, as well as statutory, regulatory, or contractual requirements regarding frequency of risk assessments.

## **RA-08: SUPPLY CHAIN RISK ASSESSMENTS**

Agencies shall:

- (a) Assess supply chain risks associated with agency systems, system components, and services; and
- (b) Update the supply chain risk assessment at least annually and when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.

Supplemental Guidance: The NJCCIC, in concert with the Department of Treasury's Division of Purchase and Property, has developed a vendor security questionnaire and other tools that are to be used to assist agencies in assessing supply chain risks. Agencies should contact the NJCCIC at [riskreview@cyber.nj.gov](mailto:riskreview@cyber.nj.gov) for assistance in conducting supply chain risk assessments.

Supply chain-related events include disruption, use of defective components, insertion of counterfeits, theft, malicious development practices, improper delivery practices, and insertion of malicious code. These events can have a significant impact on the confidentiality, integrity, or availability of a system and its information and, therefore, can also adversely impact agency operations (including mission, functions, image, or reputation), agency assets, individuals, and other organizations. The supply chain-related events may be unintentional or malicious and can occur at any point during the system life cycle. An analysis of supply chain risk can help an agency identify systems or components for which additional supply chain risk mitigations are required.

## **RA-09: RISK ASSESSMENT COMPONENTS**

Risk assessments shall include the following component activities:

- (a) System Characterization – Identify and document:
  - 1. Information assets that are within scope;
  - 2. Criticality;
  - 3. Information classification; and
  - 4. Statutory, regulatory, contractual and policy requirements.
- (b) Threat Identification – Identify and document potential threats and their sources. Threats are commonly categorized as:

1. Environmental – external fires, HVAC failure/temperature inadequacy, water pipe burst, power failure/fluctuation, etc.
  2. Human – hackers, data entry, workforce/ex-workforce members, impersonation, insertion of malicious code, theft, viruses, spam, vandalism, etc.
  3. Natural – fires, floods, electrical storms, tornados, etc.
  4. Technological – server failure, software failure, ancillary equipment failure, etc. and environmental threats, such as power outages and hazardous material spills.
  5. Other – explosions, medical emergencies, misuse or resources, etc.
- (c) Vulnerability Identification - Develop a list of technical and non-technical vulnerabilities that could be exploited or triggered by potential threat-sources. Vulnerabilities can range from incomplete or conflicting policies that govern an agency's computer usage to insufficient safeguards to protect facilities that house computer equipment to any number of software, hardware, or other technical vulnerabilities.
- (d) Control Analysis - Document and assess the effectiveness of technical and non-technical controls that have been or will be implemented to minimize or eliminate the likelihood of a threat-source exploiting a vulnerability.
- (e) Likelihood Determination - Determine the overall likelihood rating that indicates the probability that a vulnerability could be exploited by a threat-source given the existing or planned security controls.
- (f) Impact Analysis - Determine the level of adverse impact that would result from a threat successfully exploiting a vulnerability.
- (g) Control Recommendations - Identify controls that could reduce the identified risks, as appropriate to the agency's systems and/or operations, to an acceptable level. Factors to consider when developing controls may include effectiveness of recommended options (i.e., system compatibility), legislation and regulation, operational impact, and safety and reliability.
- (h) Report – Document the results of the risk assessment in an official report, spreadsheet, or briefing and submit to agency management and the State Chief Information Security Officer or his/her designee for review.

Supplemental Guidance: When completing a risk assessment report, agency CISOs must apply a risk estimation methodology (either qualitative or quantitative) to measure risk levels, an estimation of the level of risk with appropriate values assigned, and an evaluation and prioritization of the risks in relation to incident scenarios and risk levels. Agency CISOs must also consider legal and regulatory risks when completing the risk assessment report.

## RA-10: RISK CONSIDERATIONS

Agencies must account for the following risks when applying security categorizations:

- (a) Health and Public Safety Risk: Loss of confidentiality, integrity or availability would jeopardize the health or safety of individuals;
- (b) Operational Risk: Loss of confidentiality, integrity, or availability could prevent an agency, an agency function, or the State from accomplishing its core functions;
- (c) Financial Risk: Loss of confidentiality, integrity, or availability would result in a loss of revenue, or criminal and civil penalties;
- (d) Legal Risk: Failure to protect against the loss of confidentiality, integrity, or availability of information as mandated by statute, regulation, and/or contract ; and
- (e) Reputation Risk: Loss of confidentiality, integrity, or availability would result in damage to the State's or a State agency's reputation.
- (f) For all major applications and systems and general support systems, the information owner or his/her designee shall complete a System Security and Privacy Plan (SSPP) that categorizes the information:
  - (1) Prior to production implementation of new major systems and applications or general support systems;
  - (2) When substantive changes have occurred in a major system or application or general support systems;
  - (3) After a breach of system's information security controls; and
  - (4) When substantive changes have occurred in the agency information technology or organizational environments;
- (g) In accordance with the State of New Jersey [Technology Circular 195 – Contingency Planning Policy, Policy NO. 14-31-NJOIT](#), as well as the information security Contingency Planning requirements contained in this manual, complete a [Business Impact Assessment \(BIA\)](#);
- (h) Ensure the SSPP and BIA are reviewed and approved by the Agency CIO; and
- (i) Submit the SSPP and BIA as part of the NJOIT [System Architecture Review \(SAR\)](#) process for review.

Supplemental Guidance: The SSPP documents the controls and safeguards that are implemented to mitigate risks to the confidentiality, integrity, privacy, and availability. The SSPP facilitates the development of inventories of information asset mappings to specific system components where information is processed, stored, or transmitted.

The BIA provides a method for determining the impact of any disruption to agency operations due to the loss of availability of an information system.

## **RA-11: USE OF ALL-SOURCE INTELLIGENCE IN ASSESSING RISK**

Agencies shall ensure individuals within the agencies who are responsible for Information Technology, Information Security, and Privacy:

- (a) Register as members of the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC);
- (b) Subscribe to information security intelligence and information services in order to stay aware of emerging threats and vulnerabilities; and
- (c) Use the information gained from these subscriptions to update their security posture and vulnerability and patch management activities, as applicable.

Supplemental Guidance: The NJCCIC acts as the State's clearinghouse for threat intelligence and produces intelligence products including, but not limited to: alerts, bulletins, and best practices. The NJCCIC communicates agency-specific threat information to each agency so that they can be aware of threats related to their programs of work, information systems, and threats that may impact organizations and the individuals they serve. Individuals can find NJCCIC registration information at: [www.cyber.nj.gov/members](http://www.cyber.nj.gov/members).

Other suggested information sources include the [US Department of Homeland Security Cybersecurity and Infrastructure Security Agency](#), the [US Computer Emergency Readiness Team \(US-CERT\)](#), as well as vendor-specific information security resources that include vulnerability and security updates for their respective products.

## **RA-12: VULNERABILITY MONITORING AND SCANNING**

In coordination with the NJCCIC, agencies shall implement proactive vulnerability identification, remediation, and patch management practices to minimize the risk of a loss of confidentiality, integrity, and availability of State information systems and information.

## **RA-13: VULNERABILITY AND PATCH MANAGEMENT**

The State Chief Information Security Officer (CISO) shall:

- (a) Develop and implement enterprise-wide technical vulnerability and patch management tools and processes;
- (b) Utilize a risk-based model for prioritizing remediation of identified vulnerabilities;
- (c) Share the results of vulnerability scans with appropriate agency personnel; and
- (d) Document vulnerability and remediation trends throughout the enterprise.

Supplemental Guidance: Risk-based prioritization includes the severity of the vulnerability should it be exploited, the sensitivity and criticality of the systems on which it exists, the ease of exploiting the vulnerability, and the likelihood that the vulnerability will be exploited. Vulnerabilities on public-facing assets are generally prioritized for remediation due to their exposure.

Agencies should subscribe to vendor and other security mailing lists to receive notifications of vulnerabilities, patches, and other current security information on the products they employ. The NJCCIC regularly publishes vulnerability alerts as standalone threat intelligence products and within the weekly NJCCIC Bulletin.

## **RA-14: VULNERABILITY SCANNING AND REMEDIATION**

As vulnerability scanning can negatively impact network and system performance, agencies shall coordinate independent vulnerability scanning efforts with the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC).

- (a) The NJCCIC maintains licenses for enterprise vulnerability scanning and endpoint detection and response software that is to be installed on all agency endpoints and workloads to facilitate continuous vulnerability identification and remediation. The NJCCIC also manages the weekly scanning of all public-facing assets for vulnerabilities.
- (b) The NJCCIC's vulnerability scanning and monitoring tools aid in:
  - 1. Enumerating platforms, software flaws, and improper configurations;
  - 2. Measuring vulnerability impact; and
  - 3. Providing patch and remediation guidance.
- (c) Agencies are responsible for remediating legitimate vulnerabilities in accordance with an assessment of their risk. In the event that a vulnerability cannot be remediated, agencies shall submit an exception request and implement compensating controls to appropriately manage the risk.

Supplemental Guidance: Security categorization of information and information systems guides the frequency and comprehensiveness of vulnerability monitoring (including scans). Agencies, in coordination with the NJCCIC, determine the required vulnerability monitoring for system components, ensuring that the potential sources of vulnerabilities—such as infrastructure components (e.g., switches, routers, guards, sensors), networked printers, scanners, and copiers—are not overlooked.

Vulnerability monitoring and analyses for custom software may require additional approaches, such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Agencies can use these analysis approaches in source code reviews and in a variety of tools, including web-based application scanners, static analysis tools, and binary analyzers. Vulnerability monitoring includes scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for flow control mechanisms that are improperly configured or operating incorrectly.

Host-based vulnerability scanning and endpoint detection and response software installed on agency endpoints and workloads eliminate the need for privileged access network scans for those assets. Where host-based scanning cannot be used, the NJCCIC utilizes appropriate network scanning tools and techniques. The vulnerability scanning tools implemented by the NJCCIC receive automated updates for newly discovered vulnerabilities and provide for the automation of communication of vulnerabilities on agency assets. The results from these tools may express

vulnerabilities in the [Common Vulnerabilities and Exposures \(CVE\)](#) naming convention and employ the [Open Vulnerability Assessment Language \(OVAL\)](#) to determine the presence of vulnerabilities. Sources for vulnerability information include the [Common Weakness Enumeration \(CWE\)](#) listing and the [National Vulnerability Database \(NVD\)](#). The NJCCIC's tools may also express vulnerability impact by the [Common Vulnerability Scoring System \(CVSS\)](#).

## **RA-15: SOFTWARE PATCHING AND CURRENCY**

Agencies are required to ensure that:

- (a) All system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed;
- (b) Critical security patches are installed as soon as operationally possible, but no more than thirty (30) days after the vendor's release date;
- (c) Non-critical security patches are installed within ninety (90) days of the vendor's release date; and
- (d) Only vendor-supported software is installed on agency information systems.

Supplemental Guidance: Agencies are required to ensure systems are maintained and updated to manufacturer's specifications. This helps ensure that existing solutions are operating properly throughout their lifecycles.

## **RA-16: RESPONSIBLE DISCLOSURE**

In coordination with the State Chief Information Security Officer, Agency Information Technology, Security, and Privacy Officers shall establish a public reporting channel for receiving reports of vulnerabilities in agency systems and system components.

Supplemental Guidance: The reporting channel is publicly discoverable and contains clear language authorizing good-faith research and the disclosure of vulnerabilities to the agency and the NJCCIC. To assist in the centralized receipt and coordination of remediation of publicly disclosed vulnerabilities, agencies can direct reporters to submit the disclosures to the NJCCIC at [njccic@cyber.nj.gov](mailto:njccic@cyber.nj.gov). The NJCCIC will develop and disseminate further guidance to agencies for the implementation of the public disclosure program.

## **RA-17: SECURITY TESTING AUTHORIZATION**

Prior to the scheduling, contracting, or conducting penetration tests, red team exercises, vulnerability scans, compromise assessments, and other security tests against State information systems, agency management shall coordinate and must receive explicit approval for all security testing from the State Chief Information Security Officer.

Supplemental Guidance: Penetration tests, red team exercises, compromise assessments, and vulnerability scans can have adverse collateral impacts to the performance and security of other State information systems and networks.

## **RA-18: THREAT HUNTING**

The State Chief Information Security Officer shall establish and maintain a continuous threat hunting function and capability within the NJCCIC to:

- (a) Search for indicators of compromise in State systems; and
- (b) Detect, track, and disrupt threats that evade existing controls

Supplemental Guidance: Threat hunting is an active means of cyber defense in contrast to traditional protection measures, such as firewalls, intrusion detection and prevention systems, quarantining malicious code in sandboxes, and Security Information and Event Management (SIEM) technologies and systems. Cyber threat hunting involves proactively searching State systems, networks, and infrastructure for advanced threats. The objective is to track and disrupt cyber adversaries as early as possible in the attack sequence and to measurably improve the speed and accuracy of organizational responses. Indications of compromise include unusual network traffic, unusual file changes, and the presence of malicious code. Threat hunting teams leverage existing threat intelligence and may create new threat intelligence, which is shared with peer organizations, Information Sharing and Analysis Organizations (ISAO), Information Sharing and Analysis Centers (ISAC), and relevant government departments and agencies.

The NJCCIC maintains tools and other resources to aid in threat hunting across agency systems and networks. Upon discovery of threats, the NJCCIC will notify and coordinate the response to the threat with appropriate agency personnel. As resources allow, agencies may develop their own threat hunting capabilities in coordination with the NJCCIC.

## **REFERENCES**

The requirements established in the Risk Assessment policies and standards have been derived from following:

- NIST SP 800-53r5 Program Management (PM), Risk Assessment (RA);
- NIST CSF Identify/Governance (ID.GV), Identify/Risk Assessment (ID.RA);
- NIST [Risk Management Framework](#); and
- Federal Information Processing Standards (FIPS) Publication - [Standards for Security Categorization of Federal Information and Information Systems](#)

---

# PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY (PT)

---

## PT-01: PURPOSE

The purpose of the Personally Identifiable Information Processing and Transparency policies and standards is to ensure appropriate governance, accountability, and privacy protection mechanisms are implemented by State agencies that process personally identifiable information (PII).

## KEY TERMS

**Data** - A subset of information in an electronic format that allows it to be stored, retrieved or transmitted.

**Information** - Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

**Non-Sensitive Personally Identifiable Information (PII)** - Information that is available in public sources the disclosure of which cannot reasonably be expected to result in personal harm.

**Personally Identifiable Information (PII)** - Any information about an individual maintained by an agency, including:

- (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and
- (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

**Privacy** – Freedom from unauthorized intrusion or disclosure of information about an individual.

**Privacy Officer** - Individual who is responsible for the oversight of the agency's compliance with all applicable State and Federal laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information.

**Sensitive Personally Identifiable Information (SPII)** – Personal information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

## PT-02: POLICY

In accordance with all applicable laws, executive orders, regulations, circulars, directives and policies, agencies shall implement appropriate governance, accountability and privacy protection

mechanisms throughout the life cycle of personally identifiable information (PII) they create, collect, store, use, transmit, share, and dispose.

### **PT-03: PRIVACY PROGRAM**

The State Chief Technology Officer shall appoint a Privacy Officer who is responsible for:

- (a) Coordinating the State's privacy efforts with the State Chief Information Security Officer in New Jersey Office of Homeland Security's Cybersecurity and Communications Integration Cell (NJCCIC), senior leadership in the Office of the Attorney General's Cybersecurity and Privacy Division, and agency privacy officers across the Executive Branch of New Jersey State Government;
- (b) Monitoring State and Federal privacy laws for changes that affect the State's privacy program;
- (c) Providing oversight of the State's compliance with all applicable State and Federal laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information;
- (d) Ensuring that the State's privacy practices and reports are publicly available;
- (e) Ensuring that the public has access to information about the State's privacy activities and can communicate with its officials for privacy;
- (f) Employing publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices;
- (g) Developing and implementing privacy training and awareness aimed at ensuring users understand their privacy responsibilities; and
- (h) Updating the privacy program, policies, and procedures, at least annually or upon relevant changes in the law.

### **PT-04: DISSEMINATION OF PRIVACY PROGRAM INFORMATION**

- (a) The State Privacy Officer shall maintain a central resource webpage on the State's principal public website, [www.nj.gov](http://www.nj.gov) that serves as a central source of information about the State's privacy program and that:
  - 1. Ensures that the public has access to information about the State's privacy activities and can communicate with the NJOIT Privacy Office regarding privacy-related issues;
  - 2. Ensures that the State's privacy practices and reports are publicly available; and
  - 3. Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to the privacy office regarding privacy practices.
- (b) Agencies shall ensure the State's privacy notice is posted on all agency external-facing websites, mobile applications, and other digital services.

Supplemental Guidance: The current privacy notice can be found at [www.nj.gov/privacy.html](http://www.nj.gov/privacy.html)

## **PT-05: AUTHORITY TO PROCESS PERSONALLY IDENTIFIABLE INFORMATION**

Agencies shall:

- (a) Determine and document the laws, executive orders, circulars, directives, regulations, or policies that establish the agency's authority to collect, store, process, use, disseminate, disclose and dispose of personally identifiable information (PII); and
- (b) Restrict the processing of PII to only that which is authorized.

Supplemental Guidance: The term "process" includes every step of the information life cycle, including creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal. Agencies may find their authorization to process PII as documented in the laws that mandate their business functions, privacy policies and notices, contracts, information sharing agreements, memoranda of understanding, etc.

## **PT-06: PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES**

Agencies shall:

- (a) Identify and document their purpose(s) for processing personally identifiable information;
- (b) Describe the purpose(s) in the public privacy notices and policies of the agency;
- (c) Restrict the processing of personally identifiable information to only that which is compatible with the identified purpose(s); and
- (d) Monitor changes in processing personally identifiable information and implement mechanisms to ensure that any changes are made in accordance with agency legal and business requirements.

Supplemental Guidance: Identifying and documenting the purpose of processing is a prerequisite to enabling owners and operators of the system and individuals whose information is processed by the system to understand how the information will be processed. This enables individuals to make informed decisions about their engagement with information systems and agencies and to manage their privacy interests. Once the specific processing purpose has been identified, the purpose is described in the agency's privacy notices, policies, and any related privacy compliance documentation.

## **PT-07: CONSENT**

Agencies shall Implement tools or mechanisms for individuals to consent to the processing of their personally identifiable information prior to its collection in order to help individuals' make informed decisions.

Supplemental Guidance: Consent allows individuals to make informed decisions about the processing of their information. Consent may be required by applicable State laws, executive orders, circulars, directives, regulations, policies, standards, or guidelines. Otherwise, when selecting consent as a control, agencies should consider whether individuals can be reasonably expected to understand and accept the privacy risks that arise from their authorization. When soliciting consent from individuals, agencies should consider the appropriate mechanism for obtaining consent, including the type of consent (e.g., opt-in, opt-out), how to properly authenticate and identity proof individuals and how to obtain consent through electronic means. In addition, agencies should consider providing a mechanism for individuals to revoke consent once it has been provided, as appropriate.

## **PT-08: MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION**

Agencies shall:

- (a) Limit or minimize the amount of personally identifiable information to that which is relevant and necessary to accomplish the authorized purposes of collection;
- (b) Develop, document, and implement policies and procedures that address the use of personally identifiable information;
- (c) Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; and
- (d) Review and update policies and procedures at least annually or upon any relevant changes in law.

Supplemental Guidance: The use of personally identifiable information in testing, research, and training increases the risk of unauthorized disclosure or misuse of such information. Agencies should consult with their agency privacy officer, the State Privacy Officer, and/or legal counsel to ensure that the use of personally identifiable information in testing, training, and research is compatible with the original purpose for which it was collected. When possible, agencies should use placeholder or dummy data to avoid exposure of personally identifiable information when conducting testing, training, and research.

## **PT-09: PRIVACY NOTICE**

Agencies shall provide notice to individuals about the processing of personally identifiable information that:

- (a) Is available to individuals upon first interacting with an agency, and subsequently whenever the agency's use of the PII is changed;
- (b) Is clear and easy-to-understand, and expresses information about personally identifiable information processing in plain language;
- (c) Identifies the authority that authorizes the processing of personally identifiable information;

- (d) Identifies the purposes for which personally identifiable information is to be processed; and
- (e) Includes other relevant information.

Supplemental Guidance: Additional privacy notice requirements are contained in The State of New Jersey Technology Circular, [On-Line Privacy Policy, 13-09-OIT](#). The privacy notice enables individuals to understand how the agency uses PII generally and, where appropriate, to make an informed decision prior to providing PII to the agency.

## **PT-10: SPECIFIC CATEGORIES OF PERSONALLY IDENTIFIABLE INFORMATION**

Consistent with applicable State and Federal laws, regulations, executive orders, circulars, State policies and risk assessments, Agencies shall apply processing conditions and/or protections for specific categories of personally identifiable information.

When an information system processes Social Security numbers, agencies shall:

- (a) Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to their use as a personal identifier;
- (b) Not deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his or her Social Security number; and
- (c) Inform any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

Supplemental Guidance: Agencies should consult with their privacy officer and legal counsel regarding any protections that may be necessary.

## **PT-11: PERSONALLY IDENTIFIABLE INFORMATION QUALITY MANAGEMENT**

Agencies shall develop and document policies and procedures for:

- (a) Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle;
- (b) Correcting or deleting inaccurate or outdated personally identifiable information;
- (c) Disseminating notice of corrected or deleted personally identifiable information to individuals or other appropriate entities; and
- (d) Appeals of adverse decisions on correction or deletion requests.

Supplemental Guidance: Personally identifiable information quality management includes steps that agencies take to confirm the accuracy and relevance of personally identifiable information throughout the information life cycle. The information life cycle includes the creation, collection,

use, processing, storage, maintenance, dissemination, disclosure, and disposition of personally identifiable information.

The agency privacy officer is responsible for ensuring that practical means and mechanisms exist and are accessible for individuals or their authorized representatives to seek the correction or deletion of personally identifiable information.

## REFERENCES

The requirements established in the Personally Identifiable Information Processing and Transparency policies and standards have been derived from the following:

NIST SP 800-53r5 Personally Identifiable Information Processing and Transparency (PT), Program Management (PM); Media Protection (MP);

NIST CSF Identify/Governance (ID.GV);

State of New Jersey Technology Circular, [On-Line Privacy Policy, 13-09-OIT](#); and

State of New Jersey [Privacy Notice](#).

---

# MEDIA PROTECTION

---

## MP-01: PURPOSE

The purpose of the Media Protection policies and standards is to ensure that data and information, in all forms and mediums, are protected throughout their lifecycles based on their sensitivity, criticality, and value, and the impact that a loss of confidentiality, integrity, availability, and privacy would have on the agency, the State, or individuals.

## KEY TERMS

**Access-** The ability to make use of any information system or resource.

**Data** - A subset of information in an electronic format that allows it to be retrieved or transmitted.

**Information** - Any communication or representation of knowledge, such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

**Media** - Physical devices or writing surfaces including, but not limited to: magnetic tapes, optical disks, magnetic disks, Large Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

**Portable Storage Device** – An information system component that can be inserted into and removed from an information system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain non-volatile memory).

**Record** – According to the State of New Jersey Open Public Records Act, P.L. 2001, CHAPTER 404 N.J.S. 47:1A-1 et seq., a "Government record" or "record" means any paper, written or printed book, document, drawing, map, plan, photograph, microfilm, data processed or image processed document, information stored or maintained electronically or by sound-recording or in a similar device, or any copy thereof, that has been made, maintained, or kept on file in the course of his or its official business by any officer, commission, agency or authority of the State or of any political subdivision thereof, including subordinate boards thereof, or that has been received in the course of his or its official business by any such officer, commission, agency, or authority of the State or of any political subdivision thereof, including subordinate boards thereof. The terms shall not include inter-agency or intra-agency advisory, consultative, or deliberative material.

According to N.J.S.A. 47:3-20, a "Record" or "records" means: pursuant to P.L. 1953, c.410, § 2 as amended by P.L. 1994, c.140, § 3 (N.J.S.A 47:3-16), any paper, written or printed book, document or drawing, map or plan, photograph, microfilm, data processed or image processed document, sound-recording or similar device, or any copy thereof which has been made or is required by law to be received for filing, indexing, or reproducing by any officer, commission, agency or

authority of the State or of any political subdivision thereof, including subordinate boards thereof, or that has been received by any such officer, commission, agency or authority of the State or of any political subdivision thereof, including subordinate boards thereof, in connection with the transaction of public business and has been retained by such recipient or its successor as evidence of its activities or because of the information contained therein.

**Media Sanitization** - A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.

## **MP-02: POLICY**

Agencies shall implement appropriate processes and controls necessary to protect data and information in any medium or form (e.g. paper, magnetic media, tapes, portable devices, etc.) based on the data's sensitivity and criticality. Data must be protected during the system design, development, testing, implementation, and change processes to meet the agency's confidentiality and privacy commitments.

## **MP-03: MEDIA ACCESS**

Agencies shall implement controls and processes necessary to restrict access to digital and non-digital media to authorized individuals.

Supplemental Guidance: Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm.

## **MP-04: MEDIA MARKING**

To safeguard information contained on media, agencies shall ensure digital and non-digital media is marked with appropriate information classification labels, distribution limitations, and handling caveats.

Supplemental Guidance: Media marking refers to the application or use of human-readable security attributes. Media containing only data that is classified as Public requires no marking or labels. Agencies may develop agency-specific labels that denote there are several methods for labeling information assets. Examples include: For Official Use Only (FOUO), [Traffic Light Protocol \(TLP\)](#) White/Green/Amber/Red, Law Enforcement Sensitive, etc. When media remains within the agency-controlled enclave and is not distributed or transported outside of it, media marking is optional, but recommended.

## **MP-05: MEDIA STORAGE**

Agencies shall implement controls to ensure the secure storage of digital and non-digital media. Agency management, asset custodians, and users are required to:

- (a) Physically secure all media;
- (b) Maintain strict control over the storage and accessibility of media;

- (c) Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility;
- (d) Review the location's security at least annually;
- (e) Maintain strict control over the internal or external distribution of any kind of media, including the following:
  - 1. Classify and label the media so the sensitivity of the information can be determined; and
  - 2. Send the media through a secure delivery method that can be accurately tracked.

Supplemental Guidance: Controls for physically securing media are intended to prevent unauthorized individuals from gaining access to sensitive information.

## **MP-06: MEDIA TRANSPORT**

Agencies shall implement controls and processes to:

- (a) Safeguard sensitive information stored on digital media during transport outside of controlled areas using strong encryption;
- (b) Enclose sensitive hard copy information in opaque sealed envelopes or containers;
- (c) Maintain accountability for system media during transport outside of controlled areas;
- (d) Document activities associated with the transport of system media;
- (e) Restrict the activities associated with the transport of system media to authorized personnel; and
- (f) Inform users of their responsibility and provide them with the tools and training necessary to protect agency information assets during transport outside of the agency-controlled area.

Supplemental Guidance: Information system media includes both digital and non-digital media. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers), that are transported outside of controlled areas. Controlled areas are areas or spaces for which agencies provide sufficient physical and/or procedural safeguards to meet the requirements established for protecting information and/or information systems. Physical and technical safeguards for media are commensurate with the security category or classification of the information residing on the media. Safeguards to protect media during transport include, for example, locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used.

Activities associated with transport include the actual transport, as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals from outside the organization (e.g., US Postal Service or a commercial transport or delivery service). Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel, and tracking and/or obtaining explicit

records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Agencies should maintain documentation of activities associated with the transport of information system media in accordance with assessments of risk.

### **MP-07: MEDIA USE**

Agencies shall implement physical and logical security controls, as appropriate, to protect the confidentiality and integrity of agency data information system storage media throughout the life of the storage media.

### **MP-08: PORTABLE STORAGE DEVICES**

Agencies shall implement controls and processes to restrict the use of portable storage devices, and only authorize their use to individuals, devices, and endpoints where there is a justifiable business purpose, and the use is in compliance with internal agency policies, and all applicable State and Federal laws, and regulations. The following controls shall be implemented by all agencies, users, and asset custodians to protect sensitive information and mitigate the risks of system compromise as a result of the use of portable storage devices:

(a) Agencies shall:

1. Maintain an inventory of all authorized portable storage devices;
2. Provide training to users of portable storage devices to ensure they are aware of the risks they pose, and that they are trained in how to implement cryptographic protections necessary to protect sensitive information;
3. Prohibit the connection of personal storage devices to Agency information systems; and
4. Prohibit the use of portable storage devices for which no known owner exists.

(b) Users shall:

1. Encrypt all sensitive information stored on a portable storage device using strong cryptography.
2. Diligently protect the portable storage device from loss or theft;
3. Immediately report lost or stolen portable storage devices; and
4. Securely delete all sensitive information from portable storage devices when no longer necessary.

(c) Asset custodians shall:

1. Disable the "Autorun" and "Autoplay" features on all endpoints; and
2. Ensure anti-malware software is configured to perform real-time scans of all files from external sources as the files are downloaded, opened, or executed.

Supplemental Guidance: Portable storage devices are also commonly referred to as removable media. Portable storage devices introduce significant risk to the security of State information and information systems if their use is not sufficiently controlled. On highly sensitive and critical systems, agencies should consider disabling the connection ports used by portable storage devices in order to further reduce the risks of compromise of the systems. On other sensitive systems, agencies should consider limiting the types of devices that can be used. Whitelisting software and mechanisms can be implemented to allow for the connection of only authorized makes and models of portable storage devices.

Prohibiting the use of portable storage devices for which no known owner exists mitigates the risk from malicious code being introduced into agency systems from “found” devices. Additional information and guidance on controlling the risks posed by the use of portable storage devices can be found in US CERT publication, [The Risks of Portable Devices](#).

## **MP-09: MEDIA SANITIZATION**

Before disposal or reuse, media must be sanitized in accordance with the NIST Special Publication (SP) 800-88 Revision 1, [Guidelines for Media Sanitization](#). These methods ensure that data is not unintentionally disclosed to unauthorized users.

Asset custodians and asset owners are required to document and verify media sanitization and disposal actions.

Supplemental Guidance: This control applies to all information system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include, but are not limited to, media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media, such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal.

The sanitization method to be used depends on the type of storage media, the classification and sensitivity of the data which it stores, and the purpose of the media after it is sanitized.

There are three (3) primary methods for sanitizing storage media:

**Clearing** – refers to the method of sanitizing media by overwriting user addressable storage space on the media with non-sensitive data. When media is sanitized using the clearing method, it is infeasible that the cleared data will be recoverable using commercially available data recovery tools.

**Purging** – refers to a stronger method of sanitization that protects the sanitized data from recovery even when using advanced laboratory techniques. Some methods of purging - such as the degaussing of magnetic media - will render the media unusable afterwards, whereas purging by the use of a firmware secure erase command will sanitize the media and allow for its reuse.

**Destroying** – refers to the physical destruction of the media rendering the data unrecoverable. Acceptable methods of destruction include:

- Disintegration, pulverization, melting, and incineration which will completely destroy the media and any data it contains; or
- Shredding - The shred size of the refuse should be small enough to provide reasonable assurance that the data cannot be reconstructed.

As applicable, agencies should also consider cryptographically erasing drives as a secure means of sanitization. Please see [NIST Special Publication 800-88 Revision 1 - Guidelines for Media Sanitization](#) for more information on the appropriateness of cryptographic erasure.

## **MP-10: RECORDS RETENTION**

Agencies shall implement records retention programs within their respective agencies to ensure records (e.g. data and information) are retained in accordance with the State of New Jersey, Chapter 410, Laws of 1953, [Destruction of Public Records Act](#), the [State General Records Retention Schedule](#), other applicable State and Federal laws, executive orders, circulars, litigation holds, regulations, and agency business requirements.

The storage of sensitive information that has no business value, and for which all retention requirements have expired, introduces unnecessary risks and is to be disposed of in accordance with the Media Sanitization requirements contained herein.

## **REFERENCES**

The requirements established in the Media Protection policies and standards have been derived from the following:

NIST SP 800-53 Media Protection (MP), Access Control (AC), System and Communications Protection (SC);

NIST CSF Identify/Asset Management (ID.AM), Protect/Information Protection Policies and Procedures (PR.IP), Protect/Protective Technologies (PR.PT); Protect/Access Control (ID.AC);

[NIST Special Publication 800-88 Revision 1 - Guidelines for Media Sanitization](#);

US CERT publication, [The Risks of Portable Devices](#);

State of New Jersey, Chapter 410, Laws of 1953, [Destruction of Public Records Act](#); and [State General Records Retention Schedule](#)

---

# CONFIGURATION MANAGEMENT (CM)

---

## CM-01: PURPOSE

The purpose of the Configuration Management policies and standards is to ensure that baseline configuration settings are established and maintained in order to protect the confidentiality, integrity, and availability of State information assets.

## KEY TERMS

**Configuration Baseline** - A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.

## CM-02: POLICY

Agencies shall develop, implement, and document configuration management processes that establish and maintain secure configurations for information systems throughout their life cycles.

## CM-03: BASELINE CONFIGURATIONS

Agencies shall develop, document, maintain, and apply baseline security configurations to ensure information resources introduced into the production environment are executed consistently and meet applicable statutory, regulatory, policy, and contractual compliance requirements for all agency owned or managed information systems.

Agencies are required to:

- (a) In accordance with industry standards, ensure the principle of least functionality is practiced in baseline configurations to ensure only necessary ports, protocols, and services are implemented prior to implementation into the production environment;
- (b) Required technical security controls, including but not limited to endpoint detection and response software, host-based firewalls, disk encryption, and logging are to be implemented in baseline configurations for operating systems;
- (c) Periodically review and update baseline configurations:
  1. At a minimum annually;
  2. Upon release of system and security updates and patches;
  3. When system components are installed or upgraded;
  4. After a breach of the system's information security controls; and
  5. When substantive changes have occurred in the agency information technology or organizational environments.
- (d) Develop a set of standardized images that are regularly updated and act as baseline configurations for operating systems;

- (e) Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using automated tools, such as Security Content Automation Protocol (SCAP) or the Center for Internet Security (CIS) Configuration Assessment Tool (CAT);
- (f) Retain at least two (2) previous versions of baseline configurations of the system to support rollback; and
- (g) Develop and implement baseline configurations with the minimum functionality and services, and enhanced security controls when information systems are to be used in high-risk areas, such as when traveling internationally. See Appendix B for the NJCCIC Cybersecurity Guidelines for International Travel.

Supplemental Guidance: A baseline configuration is a group of settings placed on a system before it is approved for production. Established baseline configurations ensure changes to information systems are executed consistently in the production environment. Baseline configurations for systems and system components include connectivity, operational, and communications aspects of systems. Baseline configurations are documented, formally reviewed, and agreed-upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, or changes to systems and include security and privacy control implementations, operational procedures, information about system components, network topology, and logical placement of components in the system architecture. Maintaining baseline configurations requires creating new baselines as organizational systems change over time.

## **CM-04: CONFIGURATION CHANGE CONTROL**

All technology changes to production environments must follow a standard process to reduce the risk associated with change. Agencies shall involve key business stakeholders in the change process to ensure changes are appropriately tested, validated, and documented before implementing any change on a production system.

- (a) The NJ Office of Information Technology has adopted Information Technology Infrastructure Library (ITIL) change management best practices and processes for configuration change control including:
  - 1. Request Change;
  - 2. Review Request;
  - 3. Evaluate Change;
  - 4. Approve Change;
  - 5. Coordinate Implementation; and
  - 6. Review/Close Request.
- (b) Approvals to implement a configuration change to any production information system must include explicit consideration for its security impact;

- (c) Records of configuration changes to a production system must be retained for the life of the system;
- (d) Oversight for configuration change control activities must be provided and coordinated through the NJOIT Change Advisory Board (CAB) that includes security and privacy representatives;
- (e) Changes to the information system must be tested, validated, and documented before implementing the changes on the production system;
- (f) Configuration change control must include changes to components of the information system and changes to the configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers);
- (g) Prior to implementing changes, key stakeholders are to be informed of the change, its potential impacts, and other relevant information that may impact the use of the information system;
- (h) Emergency changes, including changes resulting due to the remediation of flaws, must be included in the configuration change control process;
- (i) Upon completion of significant changes, all relevant compliance requirements, such as vulnerability scans, must be completed for all new or changed systems and networks, and security-related controls (e.g., anti-malware software) are operational after significant changes are implemented; and
- (j) Rollback procedures are to be developed as part of the change plan and implemented in the event the configuration change has adverse impacts to the production environment.

Supplemental Guidance: Configuration change control for agency systems involves the systematic proposal, justification, implementation, testing, review, and disposition of system changes, including system upgrades and modifications. Configuration change control includes changes to baseline configurations, configuration items of systems, operational procedures, configuration settings for system components, remediate vulnerabilities, and unscheduled or unauthorized changes. The CAB should be convened to review and approve major changes.

The NJCCIC maintains a state-wide subscription for Center for Internet Security benchmarks. In addition, the NJCCIC maintains enterprise licenses for automated configuration assessment tools. Agencies wishing to obtain access to the CIS security benchmarks or the licensed configuration assessment tools may contact the NJCCIC at [njccic@cyber.nj.gov](mailto:njccic@cyber.nj.gov).

## **CM-05: IMPACT ANALYSIS**

- (a) Agency personnel with security and privacy responsibilities are required to analyze changes to determine potential security and privacy impacts;
- (b) As technically and operationally feasible, agencies are should implement changes in a test environment and analyze the changes for any security or privacy impacts, prior to implementing the changes in the production environment; and

- (c) After system changes have been made, agencies must verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome regarding meeting the security and privacy requirements for the system.

Supplemental Guidance: As appropriate and based on scope of changes and potential enterprise impacts, Agency, NJCCIC, and NJOIT personnel with information security and privacy responsibilities should conduct security impact analyses to determine potential security ramifications. Security impact analyses includes assessments of risk to better understand the impact of the changes and to determine if additional security controls are required.

A separate test environment requires an environment that is physically or logically separate and distinct from the production environment. The separation must be sufficient to ensure that activities in the test environment do not impact activities in the production environment and that information in the production environment is not inadvertently transmitted to the test environment. Separate environments can be achieved by physical or logical means.

## **CM-06: ACCESS RESTRICTIONS FOR CHANGE**

Agencies are required to define, document, and implement physical and logical controls that restrict the ability to make changes to only authorized individuals.

Supplemental Guidance: Changes to the hardware, software, or firmware components of systems or the operational procedures related to the system can potentially have significant effects on the security of the systems or individuals' privacy. Therefore, Agencies permit only qualified and authorized individuals to access systems for purposes of initiating changes.

## **CM-07: CONFIGURATION SETTINGS**

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications.

- (a) Agencies shall establish, document, and implement mandatory security configuration settings that reflect the most restrictive mode consistent with their operational requirement;
- (b) Agencies are to develop baseline configurations from the following resources:
- Center for Internet Security (CIS) benchmarks:  
<https://benchmarks.cisecurity.org/downloads/benchmarks/>
  - United States government Configuration Baselines:  
<https://csrc.nist.gov/projects/united-states-government-configuration-baseline>

- NIST recommended configurations and checklists:  
<http://checklists.nist.gov/>
  - National Security Agency (NSA) configuration guides:  
<https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/index.cfm>
  - Safeguard Computer Security Evaluation Matrix (SCSEM):  
<https://www.irs.gov/uac/safeguards-program>, for systems that store, process, or transmit federal tax information (FTI).
- (c) For information assets not covered by the above resources, agencies are required to document and validate configuration settings that meet all security and operational requirements;
- (d) Any deviations from standard baseline configurations tailored to meet business or operational requirements must be documented and authorized following configuration change processes prior to introduction into production; and
- (e) Agencies are required to monitor and control changes to the configuration settings in accordance with agency policies and procedures.

Supplemental Guidance: Security-related parameters are those parameters impacting the security state of information systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: (i) registry settings; (ii) account, file, directory permission settings; and (iii) settings for functions, ports, protocols, services, and remote connections. Agencies establish organization-wide configuration settings and subsequently derive specific settings for information systems. The established settings become part of the systems configuration baseline. Common secure configurations (also known as security configuration checklists, lockdown and hardening guides, and security reference guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for information technology products and platforms as well as instructions for configuring those products or platforms to meet operational requirements.

Common secure configurations can be developed by a variety of organizations, including information technology product developers, manufacturers, vendors, federal agencies, consortia, academia, industry, and other organizations in the public and private sectors. Implementation of a common secure configuration may be mandated at the organization level, mission and business process level, system level, or at a higher level, including by a regulatory agency.

## **CM-08: LEAST FUNCTIONALITY**

Agencies shall:

- (a) Adhere to the “principle of least functionality” when configuring systems to provide only mission essential capabilities;
- (b) Prohibit or restrict the use of ports, protocols, software, and services that are not required for meeting the business function of the information system;

- (c) As technically and operationally feasible limit component functionality to a single function per device (e.g., email servers or web servers, but not both);
- (d) Disable insecure, unused or unnecessary physical and logical ports/protocols (e.g., Universal Serial Bus, File Transfer Protocol, and Hyper Text Transfer Protocol) on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling;
- (e) In accordance with agency policies, rules of behavior, access agreements regarding software program usage, configure information systems to prevent execution of unauthorized software programs;
- (f) Employ software whitelisting mechanisms to ensure only authorized software programs are executed on the information system and deny execution of all unauthorized programs;
- (g) Ensure compliance with statutory, regulatory, policy, and contractual requirements, and
- (h) Periodically review configurations to ensure least functionality is maintained.

Supplemental Guidance: Systems provide a wide variety of functions and services. Some of the functions and services routinely provided by default may not be necessary to support essential organizational missions, functions, or operations. Additionally, it is sometimes convenient to provide multiple services from a single system component, but doing so increases risk over limiting the services provided by that single component. Where feasible, Agencies limit component functionality to a single function per component. Agencies consider removing unused or unnecessary software and disabling unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of components, transfer of information, and tunneling. Agencies employ network scanning tools, intrusion detection and prevention systems, and end-point protection technologies, such as firewalls and host-based intrusion detection systems, to identify and prevent the use of prohibited functions, protocols, ports, and services.

## **CM-09: SYSTEM COMPONENT INVENTORY**

Agencies shall:

- (a) Establish procedures to identify and maintain an accurate inventory of all State-owned, leased, licensed, or managed information assets in accordance with the Office of Management and Budget's, [Asset Inventory Requirements Circular, 19-12 OMB](#). In addition to the information required by 19-12-OMB, this inventory shall include all information necessary to recover from a disaster, including the description and value of the resource, the information owner and custodian, authorized users, and the resource's security categorization.

Examples of information assets include but are not limited to:

1. Information: databases and data files, system documentation, network diagrams, user manuals, training materials, operational procedures, disaster recovery plans, archived information;

2. Software: application software, application source code, system software, development tools and utilities;
  3. Equipment: physical equipment (e.g., desktop and laptop computers, portable devices, tablets, smartphones), communication equipment (e.g., routers, switches, firewalls), magnetic and optical media (e.g., tapes and disks);
  4. Services: locally hosted and cloud computing and communications services;
  5. Vendors, vendor contacts, and vendor contracts; and
  6. Authorized users.
- (b) At a minimum, review and physically verify all inventory components on a yearly basis. More stringent review timelines may be put in place per Agency requirements.

Supplemental Guidance: Examples of information that should be recorded include:

- Information system type (e.g., server, firewall, laptop, monitor)
  - Manufacturer (e.g., Dell, Cisco, Hewlett Packard, Samsung)
  - Model and/or version number
  - Asset tag and Serial Number (if applicable)
  - IP address (if applicable)
  - Information Owner/Custodian
  - Classification level (Public, Internal Use, Confidential)
  - Business criticality
  - Physical location and details of the virtual environment (if applicable)
  - License information and details regarding ownership, expiration and maintenance (if applicable)
  - End-of-support/end-of-life date (if applicable)
- (c) As technically and operationally feasible, employ automated mechanisms to help maintain current inventories of information assets. The NJCCIC requires its approved endpoint detection and response software to be installed on all State agencies' endpoints and workloads. This software can provide current inventory information including: the make/model of the device on which it is installed, the operating system and configuration of the device, and all software installed; and
- (d) Prevent duplicate accounting of system components using a centralized inventory management system.

Supplemental Guidance: System components are discrete, identifiable information technology assets that include hardware, software, and firmware. Agencies may choose to implement centralized system component inventories that include components from all organizational systems. In such situations, Agencies ensure that the inventories include system-specific information required for component accountability. The information necessary for effective accountability of system components includes the system name, software owners, software version numbers, hardware inventory specifications, software license information, and for networked components, the machine names and network addresses across all implemented

protocols (e.g., IPv4, IPv6). Inventory specifications include date of receipt, cost, model, serial number, manufacturer, supplier information, component type, and physical location.

## **CM-10: CONFIGURATION MANAGEMENT PLAN**

Agencies shall develop, document, and implement a configuration management plan for information systems that:

- (a) Addresses the roles, responsibilities, and configuration management processes and procedures;
- (b) Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
- (c) Defines the configuration items for the system and places the configuration items under configuration management;
- (d) Is reviewed and approved by agency management; and
- (e) Protects the configuration management plan from unauthorized disclosure and modification.

Supplemental Guidance: Configuration management activities occur throughout the system development life cycle. As such, there are developmental configuration management activities (e.g., the control of code and software libraries) and operational configuration management activities (e.g., control of installed components and how the components are configured). Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual systems. Configuration management plans define processes and procedures for how configuration management is used to support system development life cycle activities.

Configuration management plans are generated during the development and acquisition stage of the system development life cycle. The plans describe how to advance changes through change management processes; update configuration settings and baselines; maintain component inventories; control development, test, and operational environments; and develop, release, and update key documents.

Agencies can employ templates to help ensure the consistent and timely development and implementation of configuration management plans. Templates can represent a configuration management plan for the agency with subsets of the plan implemented on a system by system basis. Configuration management approval processes include the designation of key stakeholders responsible for reviewing and approving proposed changes to systems, and personnel who conduct security and privacy impact analyses prior to the implementation of changes to the systems. Configuration items are the system components, such as the hardware, software, firmware, and documentation to be managed.

## **CM-11: SOFTWARE USAGE RESTRICTIONS**

Agencies are required to:

- (a) Inform employees, contractors and other third parties of acceptable and unacceptable practices related to the installation and use of software, including opensource software to ensure all licensing agreements and copyright laws are observed;
- (b) Implement controls to ensure users utilize software in accordance with copyright laws and license agreements;
- (c) Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
- (d) Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Supplemental Guidance: The software inventory system should be correlated to the hardware asset inventory, so all devices and associated software are tracked from a single location. Tracking systems can include, for example, simple spreadsheets or fully automated, specialized applications depending on agency needs.

## **CM-12: USER INSTALLED SOFTWARE**

Agencies shall:

- (a) Establish policies governing the installation of software by users;
- (b) Monitor for compliance and as technically feasible, implement automated control mechanisms that restrict users from installing software;
- (c) To the greatest extent possible, ensure installed software programs are free of malicious code.

Supplemental Guidance: If provided with the necessary privileges, users have the ability to install software on agency information systems. To maintain control over the types of software installed, agencies should identify permitted and prohibited actions regarding software installation. Permitted software installations may include, for example, updates and security patches to existing software and downloading applications from organization-approved "app stores." Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that agencies consider potentially malicious. Policy enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both. See the use of the Rules of Behavior/Acceptable Use requirements included in this manual regarding prohibitions from installing, downloading, or running software that has not been approved following appropriate review in accordance with State procurement policies.

## **CM-13: INFORMATION LOCATION**

Agencies shall:

- (a) Identify and document the location of all sensitive information and information assets

and the specific system components on which the information is processed and stored;

- (b) Identify and document the users who have access to the system and system components where the information is processed and stored;
- (c) Ensure all sensitive information is stored in the United States; and
- (d) Document changes to the location (i.e., system or system components) where the information is processed and stored.

## **REFERENCES**

The requirements established in the Configuration Management policies and standards have been derived from following:

NIST SP 800-53 Configuration Management (CM), System and Information Integrity (SI); System and Communications Protection (SC);

NIST CSF Protect/Information Protection Policies and Procedures (ID.PR); and

New Jersey Department of Treasury, Office of Management and Budget, [Asset Inventory Requirements Circular, 19-12 OMB](#).

---

## ACCESS CONTROL (AC)

---

### AC-01: PURPOSE

The purpose of the Access Control policies and standards is to establish security requirements and ensure the appropriate mechanisms are provided for the control, administration, and tracking of access to, and the use of, State information assets.

### KEY TERMS

**Access** – The ability to make use of any information system or resource.

**Authenticator** - The means used to confirm the identity of a user, process, or device (e.g., user password or token).

**Bring Your Own Device (BYOD)** – The policy of permitting employees and contractors to use personally owned or third-party owned mobile devices (e.g. tablets and smart phones) for State business purposes.

**External Information System (or Component)** - An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

**Laptop Computer** - A portable computer, small enough to rest on the user's lap and having a screen that closes over the keyboard like a lid. A laptop computer has a computer operating system, and often more robust data storage and peripheral connection capabilities.

**Identifier** - Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers.

**Least Privilege** - The principle of least privilege states that only the minimum access necessary to perform an operation should be granted to a user, a process, or a program, and that access should be granted only for the minimum amount of time necessary. Least privilege is also commonly referred to as least functionality.

**Mobile Application Management (MAM)** - Mobile application management (MAM) and mobile application store (MAS) management perform application monitoring, reporting, security, and deployment.

**Mobile Device** – For the purposes of this Policy, a mobile device is defined as any smartphone or tablet device that transmits, stores, and receives data, text, and/or voice with a connection to a wireless LAN and/or cellular network.

**Mobile Device Management (MDM)** - Software that allows IT administrators to control, secure, and enforce policies on smartphones, tablets and other endpoints.

**Portable Storage Device** - An information system component that can be inserted into and removed from an information system, and that is used to store data or information (e.g., text,

video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain non-volatile memory).

**Public Information** - Information that is intended, or required, to be shared with the public.

**Sensitive information** – A term to describe any information which requires protection from unauthorized access or disclosure.

**Smartphone** - A handheld mobile communication device with a mobile operating system and an integrated mobile broadband cellular network and Wi-Fi connection capability used for voice and data communications.

**Tablet** – An open-faced handheld mobile communication and computing device with a mobile operating system, a touchscreen display, and an integrated Wi-Fi network capability. In some cases, tablets include cellular network connection capability. Tablets resemble smartphones with the major differences being that tablets are not typically used for voice communications and they are larger in size.

**User-ID** - A unique symbol or character string used by an information system to identify a specific user.

## **AC-02: POLICY**

Agencies shall establish procedures that effectively control and restrict access to agency information assets to authorized users based on defined business and legal requirements (essentially, access will be limited to a “need-to-use” and/or “need-to-know” basis). Mechanisms are required to be implemented that provide for the control, administration, and tracking of access to, and the use of, agency information assets, as well as the protection of such assets from unauthorized or unapproved activity and/or destruction.

## **AC-03: ACCOUNT MANAGEMENT**

Agencies shall:

- (a) Define and document the types of accounts (e.g. individual, shared, group, system, guest, anonymous, emergency, developer, temporary, and service) allowed and those specifically prohibited for use within the system;
- (b) Assign account managers and backup account managers for their information systems;
- (c) Establish conditions for group and role membership. Agencies shall specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
- (d) Specify:
  1. Authorized users of the system;
  2. Group and role membership; and
  3. Access authorizations (i.e., privileges) and attributes, as required for each account.

- (e) Require employee screening and background checks be completed in accordance with State and Federal laws, executive orders, circulars, regulations, directives, contractual requirements, or other policies prior to providing non-privileged and privileged access to agency information systems;
- (f) As technically feasible, agencies shall employ automated mechanisms to support management of information system accounts;
- (g) Create, enable, modify, disable, and remove information system accounts in accordance with documented agency account management procedures;
- (h) Automatically audit account creation, modification, enabling, disabling, and removal actions;
- (i) Disable:
  - 1. New accounts that have not been logged into for thirty (30) days or more;
  - 2. Accounts that have expired;
  - 3. Accounts that are no longer associated with a user;
  - 4. Accounts that have been inactive for ninety (90) days or more; and/or
  - 5. And accounts that are in violation of State/Agency policies.
- (j) As technically feasible, the information system shall automatically disable accounts per the conditions above;
- (k) Configure the information system to automatically audit account creation, modification, enabling, disabling, and removal actions, and forward the audit events to the NJCCIC for review and analysis;
- (l) Require that users log out when no longer using the information system; and
- (m) Disable accounts of individuals who pose a significant security and/or privacy risk and for which reliable evidence indicates either the intention to use authorized access to systems to cause harm or through whom adversaries will cause harm.

Supplemental Guidance: Examples of system account types include individual, shared, group, system, guest, anonymous, emergency, developer, temporary, and service. Identification of authorized system users and the specification of access privileges reflect the requirements in other controls in the security plan. Users requiring administrative privileges on system accounts receive additional scrutiny by agency personnel responsible for approving such accounts and privileged access, including system owner, information security officer, or privacy officer. Types of accounts that organizations may wish to prohibit due to increased risk include shared, group, emergency, anonymous, temporary, and guest accounts.

Agencies may choose to define access privileges or other attributes by account, type of account, or a combination of the two. Examples of other attributes required for authorizing access include restrictions on the time of day, day of week, and point of origin.

Automated system account management includes using automated mechanisms to create, enable, modify, disable, and remove accounts; notify account managers when an account is created, enabled, modified, disabled, or removed, or when users are terminated or transferred; monitor system account usage; and report atypical system account usage. Automated mechanisms can include internal system functions and email, telephonic, and text messaging notifications.

#### **AC-04: REQUIREMENTS FOR ACCOUNT REGISTRATION AND CREATION**

Agencies shall establish and document formal account creation and registration processes to include the following:

- (a) Agencies shall ensure that each User-ID generated is unique;
- (b) User-IDs should be granted to specific users only, and should not be used by anyone but the individuals to whom they have been issued;
- (c) The use of group accounts and shared IDs is generally prohibited. The use of such accounts shall require prior approval by the agency Chief Information Security Officer or his/her designee
- (d) The creation of an individual user account shall require a written or electronic request from an appropriate authorized manager, and/or Human Resources representative;
- (e) Access to information assets, systems, and services shall be provided in accordance with a user's job description/function/role on a "need-to-know" and/or "need-to-use" basis (access should correspond to the minimum amount of privilege necessary for an individual user's proper job function/duties/requirements and not necessarily their job title);
- (f) User-ID's shall not give any indication of the user's privilege level (i.e., Administrator);
- (g) User accounts should be created in such a way as to facilitate their periodic review by the Agency information security personnel and asset custodians;
- (h) Access control rules and rights for each user or group of users shall be defined and documented;
- (i) Establish and implement administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
- (j) The initial authentication factor (password) shall be valid only for the user's initial login to the system or application;
- (k) The user account shall be disabled if the initial password is not used within thirty (30) days;
- (l) The user shall be forced to change the password before completion of the initial login sequence; and

- (m) Before any third-party vendor or contractor is given access to agency information assets, a contract defining the terms and conditions of such access should be signed by the third-party vendor or contractor.

## **AC-05: REQUIREMENTS FOR PRIVILEGED ACCESS**

Agencies shall restrict and control the allocation and use of privileged user accounts.

- (a) Privileged accounts shall be limited to the minimum number required for successful management and operation of the agency information systems;
- (b) The allocation of privileged access shall be provided on a “need-to-use” and/or “need-to-know” basis (privileges should correspond to the minimum amount of privilege necessary for an individual user’s proper job function/duties/requirements and not necessarily their job title);
- (c) The process for granting privileged access shall follow the same requirements as the user registration process;
- (d) Privileged access shall be used only for duties that require escalated privileges;
- (e) Privileged access shall be audited and logged at all times;
- (f) Privileged access shall be protected and granted in such a way as to ensure that actions conducted while using privileged access can be traced to a unique user account;
- (g) Individuals with privileged access shall be required to receive special training related to the privileged access roles and responsibilities; and
- (h) Where technically feasible, or otherwise required by policy, executive order, circular, statutory, regulatory, or contractual requirement, advanced authentication methods such as multi-factor authentication, biometrics, etc., are to be used for privileged access accounts.

Supplemental Guidance: A privileged account is generally defined as a system administrator account. Privileged accounts have elevated permissions than non-privileged user accounts. Examples of privileged accounts include those that have root access, system administrator access, and accounts associated with database ownership, and network device management.

## **AC-06: REQUIREMENTS FOR TEMPORARY OR EMERGENCY ACCESS**

Temporary or emergency accounts may be established by agencies to support specific business functions for which such access is required.

- (a) Agencies shall develop procedures to properly authorize temporary or emergency access accounts, including documenting their creation and deletion when no longer needed;
- (b) Agencies shall apply password and authentication controls for temporary and emergency accounts commensurate with the role – user or administrator – required by the Identification and Authentication Policy as documented in this Manual and in accordance with other policy, contractual, and statutory requirements. Any deviation from the

password and authentication requirements shall require approval by the Agency Chief Information Security Officer; and

- (c) As technically feasible, agencies shall implement automated processes to disable temporary and emergency access accounts when no longer needed.

Supplemental Guidance: Temporary accounts may include those required for audits, software installation, software development, training, testing or another agency-approved function. Management of temporary and emergency accounts includes the removal or disabling of such accounts automatically after a predefined time period rather than at the convenience of the system administrator. Automatic removal or disabling of accounts provides a more consistent implementation.

## **AC-07: ACCESS ENFORCEMENT**

Agencies shall:

- (a) Enforce approved authorizations for role-based access to information and system resources in accordance with applicable access control policies; and
- (b) As applicable and required by law, executive order, circular, directive, or policy, provide individuals with the ability to review the personally identifiable information about them held within agency systems.

Supplemental Guidance: Role-Based Access Control (RBAC) is required when available; however, other methods to securely access files and documents may be used as appropriate, such as attribute-based access control (ABAC) or lattice-based access control (LBAC). Access control policies control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational systems.

Agency personnel should consult with their agency's privacy officer and legal counsel with respect to providing an individual with the ability to review the PII an agency holds about them.

## **AC-08: INFORMATION FLOW ENFORCEMENT**

Agencies shall:

- (a) Enforce approved authorizations for controlling the flow of information within the system and between connected systems; and
- (b) Enforce approved information flows using appropriate administrative, physical, and technical controls.

Supplemental Guidance: Information flow control regulates where information can travel within a system and between systems (in contrast to who is allowed to access the information) and without regard to subsequent accesses to that information. Information flow control mechanisms include, but are not limited to implementing:

- (a) Policies and processes;

- (b) Network segmentation and border protection mechanisms (e.g. firewalls, routers, switches, etc., to enforce flow between networks);
- (c) Conditional access and network access control mechanisms;
- (d) Role- and device-based access controls (e.g. conditional access and network access controls);
- (e) Security tools and technologies (e.g. intrusion prevention systems, web- and email-filtering solutions; endpoint detection and response software, data loss prevention tools, host-based firewalls, etc.);
- (f) Physical separation (e.g. air-gapped systems);
- (g) Domain-based Message Authentication, Reporting & Conformance (DMARC); and
- (h) Geofencing mechanisms.

Supplemental Guidance: Flow control restrictions include blocking external traffic that claims to be from within the organization, keeping sensitive information from being transmitted in the clear to the Internet, restricting web requests that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content.

## **AC-09: SEPARATION OF DUTIES**

Agencies shall:

- (a) Identify and document functions, tasks, and responsibilities including system maintenance, day-to-day computer operations, and security/system administration duties; and
- (b) Define system access authorizations to support separation of duties to prevent malevolent activity without collusion.

Supplemental Guidance: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes dividing mission or business functions and support functions among different individuals or roles, conducting system support functions with different individuals, and ensuring that security personnel who administer access control functions do not also administer audit functions.

## **AC-10: LEAST PRIVILEGE**

Agencies shall:

- (a) Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks; and
- (b) Enforce the principle of least privilege by:
  1. Limiting privileged accounts to the minimum number required for successful management and operation of agency information systems;

2. Requiring users of information system accounts, or roles to use non-privileged accounts or roles when accessing non-privileged functions;
3. Explicitly authorizing access to security functions and security-relevant information to authorized individuals or roles (e.g. system administrators, security administrators, and other appropriate privileged users). Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists;
4. Requiring individuals to use non-privileged accounts or roles when accessing non-security functions;
5. Configuring Information systems to prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures;
6. As technically and operationally feasible, requiring users to log into networked systems via local network and remote access using a non-privileged account, and escalating to a privileged account after successful authentication with the non-privileged account;
7. Auditing the use of privileged functions to detect misuse; and
8. Reassigning or removing privileges, if necessary, to correctly reflect evolving business needs.

Supplemental Guidance: Agencies are to employ the principle of least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from accessing privileged information or privileged functions. Requiring the use of non-privileged accounts when accessing non-security functions limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where agencies implement access control policies, such as role-based access control, and where a change of role provides the same degree of assurance in the change of access authorizations for the user and the processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.

## **AC-11: UNSUCCESSFUL LOGON ATTEMPTS**

Asset Custodians shall configure systems to enforce a limit of five (5) consecutive unsuccessful logon attempts by a user within a 90-minute time period. When the maximum number of unsuccessful attempts is exceeded, the system will automatically:

- (a) Lock the account or node for a 30-minute period or until the account is released by:
  1. An administrator,

2. An authorized service desk member, or
3. The user via an agency-defined challenge question or password reset process.

(b) Log all unsuccessful logon attempts and password resets;

For mobile devices: asset custodians shall configure systems to enforce a limit of five (5) consecutive invalid logon attempts by a user within a 90-minute time period. When the maximum number of unsuccessful attempts is exceeded the system will automatically:

(c) Delay the next logon prompt;

(d) Lock the account or node for a 30-minute period or until the account is released by:

1. An administrator,
2. An authorized service desk member, or
3. The user via an agency-defined challenge question process.

(e) Purge the device after ten (10) consecutive failed logon attempts.

Supplemental Guidance: The need to limit unsuccessful logon attempts and take subsequent action when the maximum number of attempts is exceeded applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are usually temporary and automatically release after a predetermined, agency-defined time period. Agency-defined challenge question processes that may be implemented include prompting the user to answer a secret question in addition to the username and password, invoking a lockdown mode with limited user capabilities (instead of full lockout), allowing users to only log on from specified Internet Protocol (IP) addresses, requiring a CAPTCHA to prevent automated attacks, or applying user profiles such as location, time of day, IP address, device, or Media Access Control (MAC) address. If automatic system lockout or execution of a delay algorithm is not implemented in support of the availability objective, agencies should consider a combination of other actions to help prevent brute force attacks. In addition to the above actions, agencies can prompt users to respond to a secret question before the number of allowed unsuccessful logon attempts is exceeded. Automatically unlocking an account after a specified period of time is generally not permitted. However, exceptions may be required based on operational mission or business need.

## **AC-12: HUMAN REVIEWS**

To maintain effective controls over user access to information assets, agencies shall implement a formal process to review user access at least every six (6) months. The review should specifically identify and revoke access for, or remove the following:

- (a) Active User IDs that are no longer needed;
- (b) User IDs assigned to terminated users with active access;
- (c) Generic or anonymous user IDs;
- (d) Redundant or duplicate user IDs; and/or

- (e) User IDs with excessive privileges, which are no longer necessary and/or are not approved by the information custodian.

### **AC-13: SYSTEM USE NOTIFICATION**

As technically feasible, asset custodians shall configure State information systems to display an agency-defined system-use notification banner that is displayed to users before granting access to the system. The notification banner shall include privacy and security notices consistent with applicable Federal and State laws, executive orders, circulars, directives, policies, regulations, standards, and guidance and shall:

(a) State the following:

1. Users are accessing an information system owned by the State of New Jersey;
2. Information system usage may be monitored, recorded, and subject to audit;
3. Unauthorized use of the State information system is prohibited and subject to criminal and civil penalties; and
4. Use of the State information system indicates consent to monitoring and recording.

(b) Retain the notification banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to, or further access the State information system.

(c) For publicly accessible systems:

1. Display system use information and conditions, before granting further access to the publicly accessible system;
2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
3. Include a description of the authorized uses of the system.

Supplemental Guidance: An example of a logon banner that may be used includes the following:

*This is a State of New Jersey information system which may be accessed and used only for official government business by authorized personnel. Unauthorized access or use of this system may subject violators to criminal, civil and/or administrative action. Administrative action may include discipline, up to and including, termination of employment or contract. All information on this system may be intercepted, recorded, read, copied, or disclosed by, and to, authorized personnel for official purposes, including, criminal, civil and/or administrative investigations. Access or use of this computer system by any person, whether authorized or unauthorized, constitutes consent to these terms.*

System use notifications can be implemented using messages or warning banners displayed before individuals log in to systems. System use notifications are used only for access via logon interfaces with human users. Notifications are not required when human interfaces do not exist. Agencies may consider system use notification messages or banners displayed in multiple

languages based on agency needs and the demographics of system users. Agencies should consult legal counsel and their privacy officer to ensure the system use notification banner meets all legal requirements.

## **AC-14: DEVICE LOCK**

Agencies shall require users to implement a device lock before leaving their system unattended and requiring the user to re-authenticate to the system to disable the device lock.

Asset custodians shall configure systems to:

- (a) Prevent further access to the system by initiating a device lock after no more than fifteen (15) minutes of inactivity;
- (b) Conceal, via the device lock, information previously visible on the display with a publicly viewable image (e.g. screen saver); and
- (c) Retain the device lock until the user reestablishes access using established identification and authentication procedures.

Supplemental Guidance: Device locks are temporary actions taken to prevent logical access to agency systems when users stop work and move away from the immediate vicinity of those systems, but do not want to log out because of the temporary nature of their absences. Device locks can be implemented at the operating system level or at the application level. A proximity lock may be used to initiate the device lock (e.g., via a Bluetooth-enabled device or dongle). User-initiated device locking is behavior or policy-based and, as such, requires users to take physical action to initiate the device lock. Device locks are not an acceptable substitute for logging out of systems, such as when agencies require users to log out at the end of workdays.

## **AC-15: SESSION TERMINATION**

Asset Custodians shall configure systems to automatically log out a user and require the user to re-authenticate to re-activate the local, network, and/or remote access session if the session has been idle for more than thirty (30) minutes.

Supplemental Guidance: A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an agency system. Such user sessions can be terminated without terminating network sessions. Session termination ends all processes associated with a user's logical session except for those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events that require automatic termination of the session include organization-defined periods of user inactivity, targeted responses to certain types of incidents, or time-of-day restrictions on system use.

## **AC-16: PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION**

Agencies shall:

- (a) Identify authorized user actions that can be performed on a system without identification or authentication consistent with organizational mission and business functions; and
- (b) Document and provide supporting rationale in the security plan for the system in which user actions may not require identification or authentication.

Supplemental Guidance: Agencies may allow certain user actions without identification or authentication, including when individuals access public websites or other publicly accessible federal systems, when individuals use mobile phones to receive calls, or when facsimiles are received. Permitting actions without identification or authentication does not apply to situations where identification and authentication have already occurred and are not repeated, but rather to situations where identification and authentication have not yet occurred. Agencies may decide that there are no user actions that can be performed on agency systems without identification and authentication.

## **AC-17: REMOTE ACCESS**

Agencies shall strictly control remote access to non-public State of New Jersey networks, systems, applications, and services. Appropriate authorizations and technical security controls shall be implemented prior to remote access being established. Where there is a business need and prior agency management approval, authorized users may be permitted to remotely connect to systems, networks, and data repositories within the Garden State Network (GSN) to conduct State-related business through secure, authenticated and managed agency approved access methods.

- (a) Access to the GSN and agency internal networks via external connections from local or remote locations shall not be automatically granted with network or system access. Systems shall be available for on- or offsite remote access only after an explicit request is made by the user and approved by the manager for the system in question;
- (b) Agencies shall establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed;
- (c) Agencies are required to authorize remote access to the information system prior to allowing such connections;
- (d) All remote access sessions are to be monitored and logged;
- (e) Agencies shall require adequate security measures (e.g. anti-virus/anti-malware software, endpoint detection and response software, vendor supported operating systems and applications, with updated security patches, etc.) on client computers prior to allowing remote or adequately protected virtual private network (VPN) access. Remote access to the GSN and Agency internal networks is a privilege and may be denied to client

systems that pose unacceptable security and privacy risks to State information systems and information;

- (f) All remote access sessions to agency information systems shall require multi-factor authentication;
- (g) All users who require remote access privileges shall be responsible for the activity performed with their user credentials. User credentials shall never be shared with those not authorized to use the credentials. User credentials shall not be utilized by anyone but the individuals to whom they have been issued. Similarly, users shall be forbidden to perform any activity with user credentials belonging to others;
- (h) Remote access may be revoked at any time for reasons including non-compliance with security policies, request by the user's supervisor, or negative impact on overall network performance attributable to remote connections;
- (i) Remote access privileges shall be terminated upon an employee's or contractor's termination from service. Remote access privileges shall be reviewed upon an employee's or contractor's change of assignments and in conjunction with other regularly scheduled user account reviews;
- (j) Except for web servers or other systems where regular users are anonymous, users are prohibited from remotely logging into any state computer system or network anonymously (for example, using "guest" accounts). If users employ system facilities that allow them to change the active user ID to gain certain privileges, such as the switch user (su) command in Unix/Linux, they must have initially logged in with a User-ID that clearly indicates their identity; and
- (k) Agencies shall implement controls to prevent split tunneling for remote devices connecting to systems and networks within the GSN unless the split tunnel is necessary for conducting agency business and is securely provisioned.

Supplemental Guidance: Remote access is defined as access to State information by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet) that are not publicly accessible (e.g. agency LAN). The use of encrypted VPNs provides sufficient assurance to the agency that it can effectively treat such connections as internal networks if the cryptographic mechanisms used are implemented in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

## **AC-17.1: CENTRALIZED MANAGEMENT OF REMOTE ACCESS INFRASTRUCTURE**

Unless otherwise authorized by the State Chief Technology Officer (CTO), the New Jersey Office of Information Technology (NJOIT) shall develop, implement, and manage enterprise remote access solutions and processes that provide authorized individuals within agencies of the Executive Branch of New Jersey State Government with remote access to agency-specific information resources.

The State CTO or his/her designee(s) is responsible for:

- (a) Implementing and managing the State of New Jersey remote access infrastructure;
- (b) Limiting the number of remote access points to that which is necessary to support users that require remote access;
- (c) Documenting approved technologies and methods of remote access to State of New Jersey information systems;
- (d) Establishing usage restrictions and implementation guidance for each allowed remote access method;
- (e) Employing automated mechanisms to monitor and control remote access methods;
- (f) Enforcing requirements for remote connections to information systems; and
- (g) Immediately deactivating remote access to users, vendors, business partners, and other third parties when it is no longer needed.

Supplemental Guidance: Consistent with [Executive Order 225](#), the Office of Information Technology is responsible for providing and maintaining the information technology infrastructure (computer, network, and storage) of the Executive Branch, including all ancillary departments and agencies of the Executive Branch. Within this Manual, the stated policies and standards require agencies to implement safeguards necessary to protect information assets against a loss of confidentiality, integrity, and availability. The term “agency” includes NJOIT and all ancillary departments and agencies.

## **AC-17.2: REMOTE ACCESS SECURITY**

The following general controls shall be implemented by NJOIT and agencies that provide users with remote access to information assets to ensure remote access is effectively controlled.

- (a) Remote access to internal networks, systems, applications, or services shall only be provided through technologies and methods authorized by the State Chief Technology Officer or his/her designee(s);
- (b) All remote access sessions to agency internal networks shall be routed through NJOIT-managed network access control points;
- (c) Access to the GSN and agency internal networks via external connections from local or remote locations shall not be automatically granted with network or system access. Systems shall be available for on- or offsite remote access only after an explicit request is made by the user and approved by the manager for the system in question;
- (d) Where technically feasible, remote access sessions will be automatically monitored and controlled;
- (e) FIPS 140-2 compliant encryption techniques shall be implemented to protect the confidentiality and integrity of remote access sessions;
- (f) All remote access sessions shall require the use of multi-factor authentication;

- (g) Remote access connections to the internal networks shall be permitted only if the following criteria for the remote information system are met:
  - 1. Software patch status is current; and
  - 2. Anti-malware software is enabled and current.
- (h) As technically feasible, remote access solutions shall:
  - 1. Validate the patch level and software versions of devices attempting to connect to the agency networks; and
  - 2. Prohibit the connection from granting access until the device has the latest available security-related patches installed.
- (i) All remote access infrastructure shall be configured to force an automatic disconnect of remote access sessions after a thirty (30) minute period of inactivity;
- (j) Asset custodians shall configure VPN technologies to limit VPN sessions to internal network assets to no greater than twenty-four (24) consecutive hours before a forced disconnect and the establishment of a new session is required;
- (k) Agencies shall develop processes to limit the execution of privileged commands and only authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence;
- (l) Agencies shall develop processes to restrict remote network connections for vendors or other third parties to only when required to perform a valid business function, and must be immediately deactivated after use;
- (m) Where technically feasible, asset custodians shall configure any device in the session path to enforce, monitor, or log usage of all activities;
- (n) Asset custodians shall audit and log remote access connections and associated activities; and
- (o) Agencies shall forward all remote access logs to the NJCCIC enterprise Security Information and Event Management (SIEM) system in accordance with the Audit and Accountability Policy as documented in this Manual.

Supplemental Guidance: The purpose of establishing maximum duration for VPN sessions is to ensure security of State information assets being accessed by users. The maximum duration requirement does not apply to extranet system-system remote access connections.

Automated monitoring and control of remote access sessions allow organizations to detect cyberattacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets).

Limiting the number of access control points for remote accesses reduces the attack surface for organizations.

### **AC-17.3: REMOTE ACCESS - AGENCY LEVEL AUTHORIZATION**

Before managers and/or supervisors authorize users to perform work via a remote access arrangement, they shall do the following:

- (a) Identify the type of work to be performed through the remote access arrangement;
- (b) Limit the authorization to only resources that are necessary to carry out the remote access arrangement safely and securely;
- (c) Consider whether the needs to support the remote access arrangement can be met with less access and connectivity than provided at the main office; and
- (d) As applicable, ensure a Remote Access Agreement between the remote access user and manager is signed and maintained in the agency file.

### **AC-17.4: TRAINING OF REMOTE ACCESS USERS**

Agencies shall ensure authorized remote access users receive security training, addressing at a minimum, the following subjects:

- (a) The responsibilities outlined in this policy;
- (b) The potential enterprise risks to both the agency's information assets and the information assets of other State agencies that are interconnected and/or available to authorized users through the Agency's IT infrastructure;
- (c) Protection of authenticators, such as passwords, personal identification numbers (PINs), and hardware tokens;
- (d) Recognition of social engineering attack techniques and appropriate mitigation measures;
- (e) The consequences for disabling, altering, or circumventing the security configurations that protect State information assets; and
- (f) Security incident management and breach disclosure procedures.

Supplemental Guidance: The remote access user training is to be provided in addition to the security training requirements as documented in the Security Awareness and Training Policy.

### **AC-17.5: REMOTE ACCESS - USER RESPONSIBILITIES**

Authorized remote access users shall be responsible for the following:

- (a) Remote access users shall adhere to all applicable information security policies, standards, and procedures regarding the use of agency information assets, regardless of the work location;
- (b) Remote access users shall ensure that all computing equipment that is connected to the State IT infrastructure network for remote access purposes has been configured in accordance with the Configuration Management, and Systems and

Communications Protection, and Systems and Information Protection requirements documented herein;

- (c) Remote access users shall not connect personally-owned information assets to the State IT infrastructure at the network-level;
- (d) Remote access users shall only connect to State IT infrastructure through secure encrypted channels; and
- (e) Remote access users shall ensure that information assets used to connect to the agency IT infrastructure are physically secured.

Supplemental Guidance: Just as in a user's State office/facility, security measures cover not only information systems and technology, but all aspects of the information and information systems used by the user, including paper files, other media, storage devices, and telecommunications equipment (e.g., laptops, tablets, and smartphones) used to conduct their work duties. Remote users must keep all State property and information secure.

Remote access users are prohibited from disabling, altering, or circumventing established security controls on agency information assets used to connect to agency IT infrastructure, such as endpoint protection software (anti-virus/anti-malware), host-based firewalls, and content filtering software.

Encrypted channels may include encrypted virtual private networks (VPNs), encrypted web access, encrypted broadband, and encrypted dial-up connections. At no time may the remote access user initiate two simultaneous connections to different networks (e.g., no split tunneling and no multi-homed connection).

## **AC-18: WIRELESS ACCESS**

Unless otherwise specified by contract or written agreement:

- (a) The New Jersey Office of Information Technology (NJOIT) shall be responsible for procuring, designing, managing, implementing, monitoring, and securing the State of New Jersey Garden State Network (GSN), which provides information technology and telecommunications resources, including WAN aggregation, remote access, data center connectivity, and Internet services to Executive Branch Departments and Agencies.
- (b) Executive Branch Agencies, whether independently or through a services agreement with NJOIT, shall be responsible for the development and implementation of network and telecommunications designs, processes, and technical security controls necessary to provide authorized access to agency technology resources, in accordance with the technical standards defined by NJOIT.
- (c) Agencies, including NJOIT, shall:
  1. Establish wireless access configuration requirements, connection requirements, usage requirements, and implementation guidance for each type of wireless access;
  2. Authorize each type of wireless access to the system prior to allowing such connections;

3. Implement physical controls to protect wireless access points from tampering;
4. Implement strong encryption for authentication and transmission; and
5. Disable wireless networking capabilities embedded within system components prior to issuance and deployment when there is no business need for the system.

Supplemental Guidance: Wireless technologies include microwave, packet radio (ultra-high frequency or very high frequency), 802.11x, and Bluetooth. Wireless networks use authentication protocols that provide authenticator protection and mutual authentication. Wireless networking capabilities represent a significant potential vulnerability that can be exploited by adversaries. To protect systems with wireless access points, strong authentication of users and devices along with strong encryption can reduce susceptibility to threats by adversaries involving wireless technologies. For similar reasons, disabling wireless capabilities when not needed for essential agency missions or business functions can reduce susceptibility to threats by adversaries involving wireless technologies.

## **AC-19: USE OF EXTERNAL SYSTEMS**

External systems are systems that are used by but not part of the agency's systems, and for which the agency has no direct control over the implementation of required controls or the assessment of control effectiveness. External information systems include, but are not limited to: personally owned computers, personally owned mobile computing devices (e.g. Bring Your Own Device (BYOD)); privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, shopping malls, or airports); information systems owned or controlled by third-party contractors or commercial entities; information systems owned or controlled by other governmental (Federal, State, or Local) organizations; and cloud computing services that are accessed from agency information systems.

Agencies shall:

- (a) Establish specific terms and conditions for the use of external systems, consistent with all applicable State and Federal laws, executive orders, circulars, the security and privacy policies and standards included in this Manual, and other agency security policies and procedures, that address the specific types of applications that can be accessed on agency systems from external systems and the highest security category of information that can be processed, stored, or transmitted on external systems;
- (b) Prohibit the use of external systems by agency personnel if the terms and conditions with the owners of the external systems cannot be established;
- (c) If the terms and conditions with the owner of the external information system are met, permit authorized individuals to use an external system to access agency systems or to process, store, or transmit agency-controlled information only after:
  1. Verification of the implementation of controls on the external system as specified in this Manual and the agency's security and privacy policies and procedures; or

2. Retains approved system connection or processing agreements with the entity hosting the external system.
- (d) Restrict or otherwise restrict the use of personal devices to process, store, and transmit agency information in accordance with the Bring Your Own Device requirements listed above;
  - (e) Prohibit the use of unapproved cloud services to process, store, or transmit agency information; and
  - (f) Restrict the use of agency-controlled portable storage devices by authorized individuals on external information systems. Limits on the use of agency-controlled portable storage devices in external information systems include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.

Supplemental Guidance: Agencies have the option to prohibit the use of any type of external system or prohibit the use of specified types of external systems, (e.g., prohibit the use of any external system that is not agency-owned or prohibit the use of personally-owned systems and devices).

For some external systems (i.e., systems operated by other organizations), the trust relationships that have been established between those organizations and the originating organization may be such that no explicit terms and conditions are required. Systems within these organizations may not be considered external. These situations occur when, for example, there are pre-existing information exchange agreements (either implicit or explicit) established between organizations or components or when such agreements are specified by applicable laws, executive orders, directives, regulations, policies, or standards. Authorized individuals include agency personnel, contractors, or other individuals with authorized access to agency systems and over which the agency has the authority to impose specific rules of behavior regarding system access. Agencies should address the use of external systems in the rules of behavior and acceptable use policies.

## **AC-20: MOBILE DEVICES**

Agencies employing mobile computing devices for State business purposes shall implement processes and security controls commensurate with the information security risks introduced by the use of mobile devices.

Supplemental Guidance: A mobile device is a computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source. Mobile device functionality may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones and tablets. Mobile devices are typically associated with a single individual. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of notebook/desktop systems, depending on the nature and intended purpose of the device. Protection and control of mobile devices is behavior or policy-based and requires users to take

physical action to protect and control such devices when outside of controlled areas. Controlled areas are spaces for which organizations provide physical or procedural controls to meet the requirements established for protecting information and systems.

### **AC-20.1: AUTHORIZATION FOR USE OF MOBILE DEVICES**

The use of mobile devices for State business purposes is at the discretion of each agency. Participating agencies shall review and authorize the use of mobile devices for State business purposes consistent with their internal policies, procedures, applicable State and Federal laws and regulations, and the policies and standards contained in this Manual.

- (a) Business Requirement: Mobile devices are provided for official State business use and may be made available or authorized for employees in positions where the associated benefits justify the additional operating costs and/or risks; and
- (b) Discretionary Approval: Approval for either providing a user with a State-owned mobile device, or allowing the use of a personally owned device for State business purposes, is at the discretion of each agency and the user's manager/supervisor.

### **AC-20.2: MOBILE DEVICE RISK ASSESSMENT REQUIREMENT**

Prior to deploying or authorizing the use of mobile devices for State business purposes, agencies must consider the risks associated with the use of mobile devices and establish processes and controls to mitigate them to acceptable levels.

Supplemental Guidance: As with all information assets, the ability to maintain the confidentiality, integrity, availability, and privacy of agency information should be the primary security objective. Agencies should consider the following threats when considering the risks associated with the use of mobile devices to conduct agency business.

Some of the threats introduced by mobile devices include:

- (a) Theft/loss of device;
- (b) Untrusted/Unsecure wireless networks;
- (c) Phishing (email), Vishing (voice), SMiShing (SMS/MMS);
- (d) Rogue apps and malware:
  1. Mobile pick-pocketing: rogue apps may access mobile device resources and carry out fraudulent activities such as the generation of premium SMSs and premium phone-calls without user intervention or approval.
  2. Stealing of personal information: theft of information such as contacts, SMSs and media files is widespread, especially on open platforms. A huge market exists for such databases.
  3. Spyware: Smartphones have features like cameras, microphones and GPS tracking. Several apps allow these features to be activated remotely without the user's knowledge.

- (e) Identity theft: This involves spoofing a phone's parameters and details. Phones can then be used as a factor for authentication;
- (f) Mobile botnets / relays: Smartphones with powerful 4G/5G connections can be used as nodes and relays in a botnet. These can be used to generate spam or launch Distributed Denial of Service (DDOS) attacks;
- (g) Espionage: Leakage of sensitive information stored on mobile devices; and
- (h) Access to app data and app user data: attention needs to be given to how applications use and store data.

### **AC-20.3: MOBILE DEVICE - BRING YOUR OWN DEVICE (BYOD)**

Agencies may opt to implement programs that allow employees and contractors to use personally owned or third-party owned mobile devices for State business purposes. Such arrangements are commonly referred to as Bring Your Own Device (BYOD). Personally owned and third-party owned mobile devices present additional risks to agencies that offer BYOD arrangements.

- (a) Agencies shall establish and implement a BYOD end-user agreement that clearly states the requirements that shall be met for a personally owned or third-party owned device to be used for State business purposes;
- (b) Personally owned and third-party owned mobile devices are subject to the same security requirements as State-owned mobile devices set forth herein, as well as any additional policies or standards as dictated by the authorizing agency;
- (c) The use of personally owned or third-party owned devices must be consistent with all applicable State and Federal laws, executive orders, circulars, regulations, and labor agreements;
- (d) Agencies offering a BYOD arrangement shall clearly state the security and support services that users of permitted personally owned mobile devices can expect. These security services may include mobile device management, password management, and remote wiping in case of loss, theft, device failure, upgrade, or change of ownership;
- (e) The BYOD policy shall clarify the systems and services allowed for use or access on a BYOD-enabled device;
- (f) Agencies offering a BYOD arrangement shall include clarifying language in the BYOD User Agreement for the expectation of privacy, requirements for litigation, e-discovery, legal holds, and records retention; and
- (g) The BYOD User Agreement shall clearly state the expectations of the loss of personal data in the event a wipe of the device is required.

### **AC-20.4: MOBILE DEVICE NETWORK ACCESS**

Agencies are to consider all personally owned and third-party owned (BYOD) network-capable mobile devices as untrusted and unsecure. Only State-owned and managed mobile devices shall be trusted and permitted to connect to internal agency networks and systems.

Supplemental Guidance: Agencies may implement guest wireless networks that are segmented from the agency's internal networks to provide network access for personally owned and third-party owned network capable mobile devices. Agencies should ensure users are aware of the prohibition against connecting personal devices to the internal agency networks and consider the use of device identification technologies and methods including 802.1X or other Network Access Control (NAC) strategies to enforce network security.

## **AC-20.5: CENTRALIZED MANAGEMENT OF MOBILE DEVICES**

Agencies deploying or authorizing the use of mobile devices for State business purposes, regardless of whether the mobile device is owned by the State, its user, or a third party, shall implement a centralized Mobile Device Management solution that is to be used to enforce the security controls and policies necessary to keep State information assets secure.

Supplemental Guidance: Centralized Mobility Management solutions may include Mobile Device Management (MDM), Mobile Application Management (MAM), or other similar solutions that allow for enforcement of security controls necessary to protect mobile devices, mobile applications, and agency data stored, accessed, processed, or transmitted on mobile devices.

MDM solutions allow for the enforcement of technical security requirements via the installation of an MDM application on the device, which provides agency IT support personnel with the ability to manage the device. MAM solutions are less intrusive to the user than MDM solutions, especially for individuals using personally owned or third-party-owned devices, as MAM only provides agency IT support personnel with the ability to manage agency application(s), the application data, and application security on the device. Both MDM and MAM solutions allow for:

- Passcode enforcement;
- AD/LDAP integration;
- Application containerization and data encryption;
- Enforcement of data loss prevention (DLP) policies;
- Jailbreak detection;
- Management of agency and commercial applications used for State business purposes; and
- Inventory tracking.

## **AC-20.6: ELIGIBLE MOBILE DEVICES**

Agencies shall only authorize the use of mobile devices for State business purposes that are capable of being managed by the agency's centralized mobility management solution and

implementing the technical security controls as required herein. Mobile devices that are incapable of being centrally managed, or of implementing the following technical controls, are not permitted to be used for State business purposes.

## **AC-20.7: MOBILE DEVICE TECHNICAL SECURITY CONTROLS**

Asset custodians shall ensure the following technical security controls are implemented and enforced on all mobile devices used for State business purposes.

- (a) Authentication - Logical access to the mobile devices and/or mobile applications that access agency data shall be controlled through the use of authenticators (passwords, biometrics, etc.);
- (b) Authenticators - Where technically feasible, mobile device passwords shall, at a minimum, consist of six (6) characters;

Supplemental Guidance: Modern mobile devices provide biometric and other advanced authentication mechanisms, in addition to device passwords. Passwords shall be established for all mobile devices used for State business purposes. The use of a biometric or alternate authenticator by the device, after the password is implemented, is permitted;

- (c) Auto-wipe - Where technically feasible, a mobile device shall automatically wipe its contents after ten (10) consecutive failed login attempts;
- (d) Session Lock - Mobile devices are required to implement an inactivity locking mechanism to lock the device and require re-authentication after no more than fifteen (15) minutes of inactivity;
- (e) Jailbreaking/Rooting - Agencies shall enforce security controls and the detection and prevention of their circumvention through the use of the centralized mobile device management system. Mobile devices that have been jailbroken/rooted shall be denied access to State information assets;

Supplemental Guidance: The terms jailbreaking and rooting are commonly referred to as the modification of a smartphone or other electronic device to remove restrictions imposed by the manufacturer or operator (e.g. to allow the installation of unauthorized software). Jailbreaking or rooting mobile devices used for State business purposes is prohibited;

- (f) Encryption - All agency non-public information stored on mobile devices shall be encrypted;

Supplemental Guidance: Modern smartphones and tablets generally offer full-device encryption as a default setting thereby protecting all data stored on them.

- (g) Anti-Malware - Anti-malware software shall be implemented on all mobile devices, where supported.
- (h) Operating System Security - Where technically feasible, all mobile devices shall have the latest available operating system updates installed upon general release by the device or operating system manufacturer.

1. Agency asset custodians are to manage operating system updates/upgrades for State-owned devices as part of their change management processes;
2. Users of BYOD mobile devices shall be responsible for implementing operating system updates on their devices;
3. Mobile devices used for State business purposes shall allow for remote validation to download the latest security patches by agency asset custodians; and
4. All mobile devices used for State business purposes shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier;

Supplemental Guidance: Mobile device operating system updates/upgrades typically include security enhancements or patches in addition to new or enhanced features. Mobile devices that are incapable of running operating systems at vendor supported levels shall be prohibited from being used for State business purposes.

- (i) Remote Wipe - All mobile devices permitted for State business use must have the capability, and be configured to allow, agency asset custodians to remotely wipe all agency non-public information.

Supplemental Guidance: This standard protects information on mobile devices if the devices are lost or stolen. On user-owned and third-party owned mobile devices, the remote wipe should only purge agency information. Personal information and applications should not be wiped. Users should note that in some cases limiting the wipe execution to only agency data may not be possible.

## **AC-20.8: INVENTORY OF MOBILE DEVICES**

Agencies shall:

- (a) Maintain an inventory of all permitted mobile devices and mobile applications that are used for State business purposes;
- (b) Permit only mobile devices that are authorized and enrolled in the agency's centralized mobility management solution for State business use; and
- (c) Record all changes to the status of these devices in the inventory.

Supplemental Guidance: Inventories should include the device manufacturer, model, operating system and patch levels, applications used for State business purposes, lost or decommissioned status, and to whom the device is assigned or approved for BYOD usage.

## **AC-20.9: APPROVED APPLICATION STORES**

To mitigate the risks associated with the installation of rogue applications, agencies shall establish a documented and communicated list of approved application stores (e.g. State/Agency App Catalog, Apple Store, Google Play, etc.) through which mobile devices may obtain approved applications.

## **AC-20.10: APPROVED APPLICATIONS**

Agencies are required to:

- (a) Establish a documented and communicated list of approved applications that may be installed and used on mobile devices that are used for State business purposes;
- (b) Establish a documented application validation process to test for device, operating system, and application compatibility issues; and
- (c) Non-approved applications shall be prohibited from being installed on State-owned mobile devices or used for State business purposes, regardless of the ownership of the device.

Supplemental Guidance: Agencies are to vet and ensure that approved applications do not introduce additional risks to the confidentiality, integrity, availability, and privacy of agency data or compromise the security of the device.

## **AC-20.11: APPLICATION MANAGEMENT**

Where technically feasible, agencies shall manage all mobile applications used for State business at the latest vendor supported levels regardless of whether the applications are installed on State-owned, user-owned, or third-party owned mobile devices.

Supplemental Guidance: Agencies are to manage security-related updates/upgrades for all State-owned devices as part of their change management processes.

## **AC-20.12: APPROVED CLOUD SERVICES**

Agencies are required to establish a documented and communicated list of approved cloud services that may be used with mobile devices used for State business purposes. The use of personal cloud services including, but not limited to, email, file storage, etc., for State business purposes is not permitted.

Supplemental Guidance: The usage of personal email accounts, personal storage accounts, and other personal cloud services is not permitted for State business purposes.

## **AC-20.13: BACKUP**

Agencies shall:

- (a) Establish mechanisms and requirements to backup mobile devices in order to mitigate the risk of loss of agency information; and
- (b) As feasible, prohibit the backing up of agency information to personal computers, personal storage devices, and personal cloud services.

## **AC-20.14: SAFETY AND COMPLIANCE**

All usage of mobile devices must comply with State, Federal, and local laws in which the mobile device is operated.

## **AC-20.15: TRAINING OF MOBILE DEVICE USERS**

Agencies shall ensure that managers, supervisors, and mobile device users receive security training, addressing at a minimum, the following subjects:

- (a) The requirements as outlined herein;
- (b) Compliance with legal, regulatory, and contractual requirements related to the use of mobile devices;
- (c) The safe use of mobile devices, especially while driving;
- (d) The potential risks to the agency's information assets;
- (e) Anti-malware awareness training, specific to mobile devices;
- (f) The potential risks associated with the use of personally owned mobile devices and the agency's limitations to support personally owned mobile devices;
- (g) The use of approved application stores and applications;
- (h) Protection of authenticators, such as passwords, personal identification numbers (PINs), and hardware tokens;
- (i) The consequences for disabling, altering, or circumventing the security configurations that protect agency information assets; and
- (j) Security incident management and loss/theft of mobile device reporting procedures.

## **AC-21: INFORMATION SHARING**

Agencies shall implement policies, procedures, and controls to protect the State's non-public information at all times.

- (a) State agencies that share data or systems must have written agreements that address the business, security, and technical requirements regarding the use and custodial responsibilities of the data and systems. These agreements can take the form of 1) a Memorandum of Agreement (MOA) or Memorandum of Understanding (MOU), Service Level Agreement (SLA), or equivalent contractual agreement, and an Interconnection Security Agreement (ISA) or 2) a combined agreement;
- (b) If the sharing of data or systems is between two state agencies as part of a service, and not otherwise governed by legal requirements, the agencies may choose to use a service level or other written agreement that clearly defines the responsibilities, services, priorities, and performance metrics of the services to be provided;
- (c) Agency software or information systems that allow the sharing of files and data

containing sensitive information shall be used to share data only if the appropriate security controls are properly configured and implemented;

(d) Appropriate security controls shall include the following:

1. Authentication controls to ensure that authorized users are identified;
2. Access controls to limit an individual's access to only the sensitive information necessary for that person to perform his/her role;
3. Authorization controls to enforce version control and record retention requirements such that only designated individuals are able to modify or delete records;
4. Audit controls that record individual actions on files and records, such as file modification;
5. Audit logs shall be retained in accordance with the agency and State records retention policies; and
6. These controls may be supplemented by operating-system-level controls (e.g., file and directory access control lists and system audit logs).

Supplemental Guidance: Information sharing applies to information that may be restricted in some manner based on some formal or administrative determination. Examples of such information include contract-sensitive information, classified information related to special access programs or compartments, privileged information, proprietary information, and personally identifiable information. Security and privacy risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to these determinations. Depending on the circumstances, sharing partners may be defined at the individual, group, agency, or state level. Information may be defined by content, type, security category, or special access program or compartment. Access restrictions may include non-disclosure agreements (NDA). Information flow techniques and security attributes may be used to provide automated assistance to users making sharing and collaboration decisions.

## **AC-22: PUBLICLY ACCESSIBLE CONTENT**

Agencies shall:

- (a) Designate individuals authorized to make information publicly accessible;
- (b) Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
- (c) Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and
- (d) Review the content on the publicly accessible system on an ongoing basis for nonpublic information and remove such information, if discovered.

Supplemental Guidance: Publicly accessible content addresses systems that are controlled by the agency and accessible to the public, typically without identification or authentication.

## REFERENCES

The requirements established in the Access Control policies and standards have been derived from the following references:

- NIST SP 800-53r5: Access Controls (AC); Identity and Authentication (IA); Configuration Management (CM); Audit and Accountability (AU); Systems and Information Protection (SI); Systems and Communication Protection (SC); and
- NIST CSF: Protect – Access Control (PR-AC).

---

## IDENTITY AND AUTHENTICATION (IA)

---

### IA-01: PURPOSE

The purpose of the Identity and Authentication policies and standards is to establish the identification, authorization, and authentication requirements necessary to ensure access to State information assets is controlled and securely provided to only authorized individuals, systems, and processes.

### KEY TERMS

**Access** – The ability to make use of any information system or resource.

**Authenticator** - The means used to confirm the identity of a user, process, or device (e.g., user password or token).

**Cryptographic Module** - The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.

**Identifier** - Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers.

**Multi-factor authentication (MFA)** - Authentication using two or more factors to achieve authentication. Factors include:

- (i) Something you know (e.g. password/PIN);
- (ii) Something you have (e.g., cryptographic identification device, token); or
- (iii) Something you are (e.g., biometric). See Authenticator.

**Public Key Infrastructure (PKI)** - A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

### IA-02: POLICY

Agencies shall establish procedures and implement identification, authentication, and authorization controls to ensure only authorized individuals, systems, and processes can access State of New Jersey information and information systems.

### IA-03: USER IDENTIFICATION AND AUTHENTICATION

Agencies shall:

- (a) Uniquely identify and authenticate users and associate that unique identification with processes acting on behalf of those users;
- (b) Implement MFA for:

1. Access to privileged user accounts;
  2. All remote access logins to agency systems that store, process, or transmit sensitive information;
  3. As technically and operationally feasible, for local logons using non-privileged user accounts; and
  4. Where MFA is not supported for local access to privileged user accounts, accounts must use at least fifteen (15) character passwords.
- (c) As technically feasible, implement replay-resistant authentication mechanisms (e.g. one-time passwords) for network access to privileged accounts;
- (d) Provide a single sign-on (SSO) capability for information system accounts; and
- (e) As applicable to agency needs, accept and electronically verify Personal Identity Verification (PIV)-compliant credentials.

Supplemental Guidance: Agencies employ passwords, physical authenticators, or biometrics to authenticate user identities or, in the case of multi-factor authentication (MFA), some combination thereof. Access to agency systems is defined as either local access or network access. Local access is any access to agency systems by users or processes acting on behalf of users, where access is obtained through direct connections without the use of networks. Network access is access to agency systems by users (or processes acting on behalf of users) where access is obtained through network connections (e.g. non-local accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks.

MFA requires the use of two or more different factors to achieve authentication.

Single sign-on (SSO) enables users to log in once and gain access to multiple system resources. Agencies must consider the operational efficiencies provided by SSO capabilities with the risk introduced by allowing access to multiple systems via a single authentication event. SSO can present opportunities to improve system security, for example, by providing the ability to add MFA for applications and systems (existing and new) that may not be able to natively support MFA.

PIV-compliant credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents.

## **IA-04: DEVICE IDENTIFICATION AND AUTHENTICATION**

As technically feasible, agencies shall:

- (a) Uniquely identify and authenticate user devices before establishing network or remote access sessions to ensure that all users connecting to agency information systems adhere to required security configurations for their devices, including the implementation of required patches and security controls and technologies .
- (b) Use only approved procedures, mechanisms, or protocols for host or device

authentication. Approved mechanisms and protocols include, but are not limited to, the following:

1. Media Access Control (MAC) address filtering;
2. Institute of Electrical and Electronics Engineers (IEEE) 802.1x and Extensible Authentication Protocol (EAP);
3. Vendor-specific solutions that provide basic identification and authentication for devices (e.g. Network Access Control, Conditional Access, Zero-Trust Network, and Mobile Device Management technologies);
4. RADIUS server with EAP-Transport Layer Security (TLS) authentication; and/or
5. Implement network routing and border protection to supplement equipment identification by allowing specific equipment to connect only from specified external networks or internal sub networks (“subnets”).

Supplemental Guidance: Agencies should determine the required strength of authentication mechanisms based on the security categories of systems and mission or business requirements. Due to the challenges of implementing device authentication on a large scale, organizations can restrict the application of the control to a limited number/type of device based on mission or business needs.

## **IA-05: IDENTIFIER MANAGEMENT**

Agencies shall implement processes to manage system identifiers (User-IDs and Device-IDs) by:

- (a) Receiving authorization from a designated agency representative (e.g. system administrator, system owner, etc.);
- (b) Selecting an identifier that identifies the individual, group, role, service, or device;
- (c) Assigning the identifier to the intended individual, group, role, service, or device;
- (d) Preventing reuse of identifiers for seven (7) years; and
- (e) Uniquely identifying each individual according to their work status (e.g. employee, contractor, etc.).

Supplemental Guidance: Common device identifiers include Media Access Control (MAC) addresses, Internet Protocol (IP) addresses, or device-unique token identifiers. Typically, individual identifiers are the usernames or User-IDs of the system accounts assigned to those individuals. Preventing the reuse of identifiers implies preventing the assignment of previously used individuals, groups, roles, services, or device identifiers to different individuals, groups, roles, services, or devices.

## **IA-06: AUTHENTICATOR MANAGEMENT**

Agencies shall implement processes that manage authenticators (e.g. passwords, tokens, biometrics, PKI certificates, and key cards) for users and devices as follows:

- (a) Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;
- (b) Establishing initial authenticator content for any authenticators issued by the agency;
- (c) Ensuring that authenticators have sufficient strength of mechanism for their intended use;
- (d) Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;
- (e) Changing default authenticators prior to first use;
- (f) Changing the initial authenticator distributed to the user upon first use;
- (g) Protecting authenticator content from unauthorized disclosure and modification;
- (h) Requiring individuals to take and having devices implement specific controls to protect authenticators; and
- (i) Changing authenticators for group or role accounts when membership to those accounts changes.

Supplemental Guidance: Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and ID badges. Device authenticators include certificates and passwords. Initial authenticator content is the actual content of the authenticator (e.g., the initial password). In contrast, the requirements for authenticator content contain specific criteria or characteristics (e.g., minimum password length). Developers may deliver system components with factory default authentication credentials (e.g., passwords) to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant risk.

## **IA-07: PASSWORD-BASED AUTHENTICATION**

As technically and operationally feasible, for password-based authentication agencies shall:

- (a) Maintain a list of commonly-used, expected, or compromised passwords and periodically update the list when passwords are suspected to have been compromised directly or indirectly;
- (b) When users create or update passwords, verify that the passwords are not found on the list of commonly-used, expected, or compromised passwords;
- (c) Only transmit passwords over cryptographically-protected channels;
- (d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;
- (e) Require immediate selection of a new password upon account recovery (e.g. forgotten password);

- (f) Allow user selection of long passwords and passphrases, including spaces and all printable characters; and
- (g) Employ automated tools to assist the user in selecting strong password authenticators.

Supplemental Guidance: Password-based authentication applies to passwords regardless of whether they are used in single-factor or multi-factor authentication. Longer passwords or passphrases are preferable over shorter passwords.

## **IA-08: PASSWORD REQUIREMENTS FOR NON-PRIVILEGED USER ACCOUNTS**

A non-privileged account is generally defined as a standard user account that does not have elevated privileges, such as administrator access to a system. For instance, non-privileged accounts cannot make configuration changes to an information system or change the security posture of a system. Agencies shall establish authentication and password requirements that meet at least the following minimum requirements for individual non-privileged user accounts used to authenticate to agency information assets. More restrictive controls may be implemented based upon the sensitivity and criticality of the information asset, or other policy, statutory, regulatory, and contractual requirements.

- (a) Passwords for individual user accounts are required to be at least eight (8) characters in length;
- (b) Passwords must not contain the user's account name or parts of the user's full name that exceed two consecutive characters;
- (c) Passwords are required to contain characters from each of the following four (4) categories:
  - (1) English uppercase characters (A through Z);
  - (2) English lowercase characters (a through z);
  - (3) Base 10 digits (0 through 9); and
  - (4) Non-alphanumeric characters (for example: !, \$, #, >, %).
- (d) Users shall be required to change their passwords at least every ninety (90) days or immediately upon the suspected compromise of the password;
- (e) Systems shall be configured to prohibit users from changing their passwords more than once in a 24-hour period. If it is necessary for a user to change a password more than once within a 24-hour period, the user will be required to contact the Agency's IT Service Desk for assistance; and
- (f) Users shall be restricted from reusing their previous twenty-four (24) passwords.

Supplemental Guidance: Passwords may exceed eight (8) characters so long as agency business processes are not negatively impacted. Passwords should never be written down or stored online in an unencrypted format.

In June of 2017, [NIST published Special Publication \(SP\) 800-63-3: Digital Authentication Guidelines](#) that provides new guidance regarding passwords. Most significantly, the guidelines remove the complexity requirement for passwords and instead focuses on password strength based on its length as an indicator of strength. The longer a password, the more entropy it has, and mathematically it will take longer to brute force guess the password. While the NIST guidelines remove the complexity requirement for passwords, the State of New Jersey password requirements shall continue to include the complexity requirement to satisfy its compliance obligations with statutory, regulatory, and contractual requirements regarding authentication.

## **IA-09: PASSWORD REQUIREMENTS FOR PRIVILEGED USER ACCOUNTS**

A privileged account is generally defined as a system administrator account. Privileged accounts have elevated permissions compared to those of a non-privileged user account. Examples of privileged accounts include ones with root access, system administrator access, and accounts associated with database ownership and network device management.

- (a) As technically feasible, passwords for privileged user accounts are required to be at least fifteen (15) characters in length;
- (b) Passwords shall not contain the user's account name or parts of the user's full name that exceed two consecutive characters;
- (c) Passwords are required to contain characters from each of the following four (4) categories:
  - (1) English uppercase characters (A through Z);
  - (2) English lowercase characters (a through z);
  - (3) Base 10 digits (0 through 9); and
  - (4) Non-alphanumeric characters (for example: ! \$ # > %);
- (d) Users of privileged user accounts shall be required to change their passwords at least every forty-five (45) days or immediately upon the suspected compromise of the password;
- (e) Systems shall be configured to prohibit users with privileged user accounts from changing their passwords more than once in a 24-hour period. If it is necessary for a user with administrative privileges to change a password more than once within a 24-hour period, the user will be required to contact the Agency's IT Service Desk for assistance;
- (f) Systems shall be configured to disallow the reuse of the previous twenty-four (24) privilege user passwords; and

- (g) All privileged user accounts shall be required to use multi-factor authentication for all local, network, and remote access to agency information systems.

Supplemental Guidance: Passwords may exceed fifteen (15) characters so long as agency business processes are not negatively impacted (Note: the maximum password length for a Windows system is 127 characters).

## **IA-10: PASSWORD REQUIREMENTS FOR SERVICE ACCOUNTS**

Service accounts are accounts used to facilitate automated processing. In general, service accounts are not user-interactive since agency personnel are not able to log on to them.

- (a) Service accounts shall only be granted the minimum level of access required to run a process.
- (b) Service accounts must be dedicated solely to their business purpose and not shared by an end user.
- (c) Service accounts shall be separate from privileged and non-privileged user accounts.
- (d) All service accounts must have appropriate logging and send logs to the NJCCIC. The asset custodian of the system on which the service account resides must audit the service account usage semi-annually, at a minimum.
- (e) Passwords for service accounts are required to be at least fifteen (15) characters in length. Passwords may exceed 15 characters so long as agency business processes are not negatively impacted.
- (f) Passwords are required to contain characters from each of the following four (4) categories:
  - (1) English uppercase characters (A through Z);
  - (2) English lowercase characters (a through z);
  - (3) Base 10 digits (0 through 9); and
  - (4) Non-alphanumeric characters (for example: ! \$ # > %).
- (g) Service account passwords are required to be changed at least every 365 days or immediately upon the suspected compromise of the password.
- (h) Systems shall be configured to prohibit service account passwords from being changed more than once in a 24-hour period. If it is necessary for a service account password to be changed more than once within a 24-hour period, the Agency's IT Service Desk must be contacted for assistance.
- (i) Systems shall be configured to restrict service accounts from reusing their previous twenty-four (24) passwords.
- (j) Service accounts shall be configured to prohibit interactive logins when technically feasible.

Supplemental Guidance: Passwords may exceed fifteen (15) characters so long as agency business processes are not negatively impacted (Note: the maximum password length for a Windows system is 127 characters).

## **IA-11: PUBLIC KEY-BASED AUTHENTICATION**

For public key-based authentication, agencies shall:

- (a) Enforce authorized access to the corresponding private key;
- (b) Map the authenticated identity to the account of the individual or group; and
- (c) When public key infrastructure (PKI) is used:
  1. Validate certificates by constructing and verifying a certification path to an accepted trust anchor (certificate authority), including checking certificate status information; and
  2. Implement a local cache of revocation data to support path discovery and validation.

Supplemental Guidance: Public key cryptography is a valid authentication mechanism for individuals, machines, and devices. For PKI solutions, status information for certification paths includes certificate revocation lists or certificate status protocol responses. For PIV cards, certificate validation involves the construction and verification of a certification path to the Common Policy Root trust anchor, which includes certificate policy processing. Implementing a local cache of revocation data to support path discovery and validation also supports system availability in situations where organizations are unable to access revocation information via the network.

## **IA-12: PROTECTION OF AUTHENTICATORS**

Agencies shall implement processes and controls to protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

Supplemental Guidance: For systems that contain multiple security categories of information without reliable physical or logical separation between categories, authenticators used to grant access to the systems are protected commensurate with the highest security category of information on the systems.

## **IA-13: AUTHENTICATION FEEDBACK**

Agencies shall ensure the authentication information is masked or otherwise obscured during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

Supplemental Guidance: Authentication feedback from systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of systems, such as desktops or notebooks with relatively large monitors, the threat (referred to as shoulder surfing) may be significant. For other types of systems, such as mobile devices with small displays, the threat may be less significant and is balanced against the

increased likelihood of typographic input errors due to small keyboards. Thus, the means for obscuring authentication feedback is selected accordingly. Obscuring authentication feedback includes displaying asterisks when users type passwords into input devices or displaying feedback for a very limited time before obscuring it.

## **IA-14: CRYPTOGRAPHIC MODULE AUTHENTICATION**

Agencies shall implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable State and Federal laws, executive orders, circulars, directives, policies, regulations, standards, and guidelines for such authentication.

Supplemental Guidance: In general, agencies are required to use [FIPS 140-2](#) approved cryptographic modules for any system, application, or device. Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role.

## **IA-15: IDENTIFICATION AND AUTHENTICATION FOR EXTERNAL USERS**

Agencies shall:

- (a) Implement mechanisms to uniquely identify and authenticate external users (e.g. general public, third-party associates, vendors, and others who are not considered State employees or contractors and have not already been provided a State/Agency user account) or processes acting on behalf of external users;
- (b) As technically and operationally feasible:
  - 1. Accept and verify third-party credentials that meet or exceed the set of minimum state and federal technical, security, privacy, and agency identity management policy requirements;
  - 2. Accept Personal Identity Verification (PIV)-compliant credentials;
  - 3. Accept NIST-compliant credentials (e.g. Secure Assertion Markup Language (SAML) assertions, and Open ID Protect 2.0); and
- (c) Document and maintain a list of accepted external authenticators.

Supplemental Guidance: This control typically applies to agency information systems (e.g. agency public-facing websites and web applications) that are accessible to the general public or third-party organizations (collectively referred to as external users).

## **IA-16: RE-AUTHENTICATION**

Asset Custodians shall configure systems to require users to re-authenticate:

- (a) Upon session termination or device lock;
- (b) After an agency-defined time period;
- (c) After a change in the user's authenticators (password reset);

- (d) Upon execution of privileged functions; and/or
- (e) Other agency security or business reason.

## **IA-17: IDENTITY PROOFING**

(a) Agencies shall:

1. Identity proof users that require accounts for logical access to systems based on the sensitivity and criticality of the information system and information, and/or requirements of applicable State and Federal laws, executive orders, directives, policies, regulations, standards, and contractual requirements;
2. Resolve user identities to a unique individual; and
3. Collect, validate, and verify identity evidence.

(b) Commensurate with the level of assurance necessary to mitigate the security and privacy risks, agencies shall implement one or more of the enhanced identity proofing processes:

1. Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization to ensure that the user's management chain is aware of the account, the account is essential to carry out organizational missions and functions, and the user's privileges are appropriate for the anticipated responsibilities and authorities within the agency;
2. Require documentary evidence or a combination of documents and biometrics be presented to reduce the likelihood of individuals using fraudulent identification to establish an identity;
3. Validate and confirm that the presented identity evidence is genuine and authentic, and the data contained in the evidence is correct, current, and related to the individual;
4. Require that the validation and verification of identity evidence be conducted in person to reduce the likelihood of fraudulent credentials being issued;
5. Deliver a registration code or notice of proofing through an out-of-band channel (e.g. delivery to home address, email address or telephone number on file) to ensure that the individual associated with an address of record is the same individual that participated in the registration; and/or
6. Accept externally-proofed identities conducted at a commensurate level of assurance by other agencies or organizations to limit unnecessary re-proofing and enable federated identities across agencies and organizations.

Supplemental Guidance: Identity proofing is the process of collecting, validating, and verifying a user's identity information for the purposes of establishing credentials for accessing a system. Identity proofing is intended to mitigate threats to the registration of users and the establishment of their accounts. The NIST standards and guidelines specifying identity assurance levels for identity proofing can be found at <https://pages.nist.gov/800-63-3/>. Agencies may be subject to

laws (e.g. Real-ID, voter registration, etc.), executive orders, directives, regulations, or policies that address the collection of identity evidence. Agencies are advised to consult with their privacy officer and legal counsel regarding such requirements.

## REFERENCES

The requirements established in the Identity and Authentication policies and standards have been derived from the following:

- NIST SP 800-53r5 Identity and Authentication (IA), Access Control (AC), Media Protection (MP);
- NIST CSF Protect/Access Controls (PR.AC); and
- NIST [Special Publication \(SP\) 800-63-3: Digital Authentication Guidelines](#).

---

## SYSTEM AND INFORMATION INTEGRITY (SI)

---

### SI-01: PURPOSE

The purpose of the Systems and Information Protection policies and standards is to ensure controls are implemented to protect State information and information systems from a loss of confidentiality, integrity, availability, and privacy.

### KEY TERMS

**Data** - A subset of information in an electronic format that allows it to be stored, retrieved or transmitted.

**Information** - Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

**Media Sanitization** - A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.

**Non-Sensitive Personally Identifiable Information (PII)** - Any information that is available in public sources and the disclosure of which cannot reasonably be expected to result in personal harm.

**Personally Identifiable Information (PII)** - Any information about an individual maintained by an agency, including:

- (3) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and
- (4) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

**Privacy** – Freedom from unauthorized intrusion or disclosure of information about an individual.

**Privacy Officer** - Individual who is responsible for the oversight of the agency's compliance with all applicable State and Federal laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information.

**Sensitive Personally Identifiable Information (SPII)** – Personal information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

### SI-02: SYSTEM AND INFORMATION INTEGRITY POLICY

Agencies shall ensure all appropriate system and information integrity controls are implemented on information systems and information consistent with their security categorization.

## **SI-03: FLAW REMEDIATION**

Agencies shall:

- (a) Identify, report, and correct system flaws;
- (b) Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
- (c) Install applicable, critical security patches as soon as operationally feasible within one (1) month of release from the vendor;
- (d) Install applicable, non-critical patches within two (2) months of release from the vendor;
- (e) As feasible automate its flaw remediation processes and activities; and
- (f) Incorporate flaw remediation into the agency configuration management process.

Supplemental Guidance: Flaw remediation is another term for security patch management and software updates. Patching and installing security updates is an essential aspect of risk management practices. Agencies should consider all risks and threats to agency information systems and information, and patch/update commensurate with those risk and threats. To aid in automating and centrally managing updates, agencies should consider using tools such as Microsoft System Security Center (SCCM), Windows Server Update Server (WSUS), Symantec Altiris, Dell KACE, Ansible, Puppet, Chef, and other patch management tools. Agencies should consult with NJOIT regarding procurement and licensing of patch management tools.

## **SI-04: MALICIOUS CODE PROTECTION**

The NJCCIC procures, implements, and manages several enterprise malicious code protection tools including endpoint detection and response, email and web filtering, intrusion prevention and detection system, web application firewalls, and others.

Agencies shall:

- (a) Ensure, at a minimum, the enterprise malicious code protection tools and technologies provided by the NJCCIC are implemented on all information systems on which the malicious code protection tools are supported to detect and eradicate malicious code;
- (b) Update the endpoint detection and response software on its endpoints and workloads in accordance with NJCCIC versioning recommendations; and
- (c) Investigate alerts and report false positives to the NJCCIC.

Supplemental Guidance: The NJCCIC suite of malicious code protection tools are automatically updated to detect and prevent new threats. As part of its responsibilities, the NJCCIC centrally manages and monitors its malicious code protection tools for alerts or other issues. Alerts and issues identified are communicated to agency security personnel for handling, as appropriate. Agencies may implement additional malicious code protection tools in concert with those provided by the NJCCIC, so long as those implemented by the agency do not conflict with or otherwise disable the enterprise security technologies.

## **SI-05: SYSTEM MONITORING**

As permissible by law and as part of its enterprise security responsibilities, the NJCCIC implements, maintains, and monitors centralized security systems including, but not limited to: anti-virus/anti-malware software, firewalls, host and network intrusion protection and intrusion detection systems, vulnerability management systems, database and application monitoring systems, data loss prevention, and web and email content filtering systems that collect, detect, and alert on:

- (a) Attacks and indicators of potential attacks;
- (b) Unauthorized local, network, and remote connections;
- (c) Rogue wireless devices;
- (d) Privileged user activity including creation, deletion, and elevation of privileges;
- (e) Unauthorized devices, applications, and network services;
- (f) System generated alerts; and
- (g) Anomalous network, application, system, and user activity.

The NJCCIC shall make access to its centralized system monitoring tools available to agencies. Agencies may augment the NJCCIC's system monitoring efforts through the implementation of its own monitoring tools to monitor its own systems and networks as permissible by law.

Supplemental Guidance: For more information and the requirements for access to the NJCCIC's system monitoring tools, agencies should contact the NJCCIC at [njccic@cyber.nj.gov](mailto:njccic@cyber.nj.gov).

## **SI-06: SECURITY ALERTS, ADVISORIES AND DIRECTIVES**

The NJCCIC shall provide State agencies with current and relevant security-related advisories, alerts, and directives on a periodic basis. Such alerts, advisories, and directives may be distributed via email, phone, text message, Internet or Intranet postings, or other communications medium, as appropriate.

Agencies shall ensure individuals within the agencies who are responsible for Information Technology, Information Security, and Privacy:

- (a) Register as members of the New Jersey Cybersecurity and Communications Integration Cell;
- (b) Subscribe to information security intelligence and information services in order to stay aware of emerging threats and vulnerabilities; and
- (c) Use the information gained from these subscriptions to update their security posture and vulnerability and patch management activities, as applicable.

Supplemental Guidance: The NJCCIC acts as the State's clearinghouse for threat intelligence and produces intelligence products including, but not limited to: alerts, bulletins, and best practices. The NJCCIC communicates agency-specific threat information to each agency so that they can be aware of threats related to their programs of work, information systems, and threats that may

impact organizations and the individuals they serve. Individuals can find NJCCIC registration information at: <https://www.cyber.nj.gov/members>.

Other suggested information sources/subscriptions include the US Department of Homeland Security [Cybersecurity and Infrastructure Security Agency](#), the [US Computer Emergency Readiness Team \(US-CERT\)](#), as well as vendor-specific information security resources that include vulnerability and security updates for their respective products.

## **SI-07: SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY**

Agencies shall:

- (a) Employ integrity verification tools to detect unauthorized changes to the system and application executables, configuration files, firmware interfaces, audit logs, and other information; and
- (b) Incorporate the detection of the unauthorized changes into the monitoring and alerting processes such that unauthorized changes are investigated.

Supplemental Guidance: Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity. Software includes operating systems (with key internal components, such as kernels or drivers), middleware, and applications. Firmware interfaces include Unified Extensible Firmware Interface (UEFI) and Basic Input/Output System (BIOS). Information includes personally identifiable information and metadata that contains security and privacy attributes associated with information. Integrity-checking mechanisms—including parity checks, cyclical redundancy checks, cryptographic hashes, and associated tools—can automatically monitor the integrity of systems and hosted applications.

## **SI-08: EMAIL AND WEB FILTERING PROTECTION**

Agencies shall:

- (a) Employ the NJCCIC and NJOIT approved email- and web-filtering solutions that detect, quarantine, and block spam, phishing emails, malicious attachments, links, and web content at all system entry and exit points to detect and act on unsolicited messages; and
- (b) Ensure users are aware of the proper use of email and the web, their risks, the actions to take to mitigate risks, and how to report suspicious emails and websites.

Supplemental Guidance: Approved email- and web-filtering solutions include those that are automatically updated to detect emerging threats, utilize artificial intelligence and signature-based detection functionality, and integrate with other State information security tools and technologies. As feasible, agencies may implement additional email and web-filtering technologies to augment those centrally managed by the NJCCIC and NJOIT, so long as they do not conflict or otherwise disable those provided by the NJCCIC and NJOIT.

Users who receive spam or other suspicious emails sent to their State email accounts should forward them to the NJCCIC at [spamreport@cyber.nj.gov](mailto:spamreport@cyber.nj.gov).

## **SI-09: INFORMATION INPUT VALIDATION**

Agencies shall implement mechanisms on agency information systems to check the validity of information inputs including character set, length, numerical range, and acceptable values required to execute job functions.

Supplemental Guidance: Checking the valid syntax and semantics of system inputs - including character set, length, numerical range, and acceptable values - verifies that inputs match specified definitions for format and content. For example, if the agency specifies that numerical values between 1-100 are the only acceptable inputs for a field in a given application, inputs of "387," "abc," or "%K%" are invalid inputs and are not accepted as input to the system. Valid inputs are likely to vary from field to field within a software application. Applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the corrupted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing them to interpreters prevents the content from being unintentionally interpreted as commands. Input validation ensures accurate and correct inputs and prevents attacks such as cross-site scripting and a variety of injection attacks.

## **SI-10: ERROR HANDLING**

Agency information systems shall only:

- (a) Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and
- (b) Reveal error messages only to designated personnel

Supplemental Guidance: Agencies must consider the structure and content of error messages. Exploitable error information includes stack traces and implementation details; erroneous logon attempts with passwords mistakenly entered as the username; mission or business information that can be derived from, if not stated explicitly by, the information recorded; and personally identifiable information, such as account numbers, social security numbers, and credit card numbers. Error messages may also provide a covert channel for transmitting information.

## **SI-11: MEMORY PROTECTION**

As technically feasible, agencies shall implement appropriate safeguards to protect system memory from unauthorized code execution.

Supplemental Guidance: Memory protection is a way to control memory access rights on a computer, and is a part of most modern instruction set architectures and operating systems. The main purpose of memory protection is to prevent a process from accessing memory that has not

been allocated to it. This prevents a bug or malware within a process from affecting other processes, or the operating system itself. Protection may encompass all accesses to a specified area of memory, write accesses, or attempts to execute the contents of the area. An attempt to access unauthorized[a] memory results in a hardware fault, e.g., a segmentation fault, storage violation exception, generally causing abnormal termination of the offending process. Memory protection for computer security includes additional techniques, such as address space layout randomization and executable space protection.

Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Controls employed to protect memory include data execution prevention and address space layout randomization. Data execution prevention controls can either be hardware-enforced or software-enforced; however, hardware enforcement provides the greater strength of mechanism.

## **SI-12: INFORMATION MANAGEMENT AND RETENTION**

Agencies shall manage and retain information within the system and information output from the system in accordance with applicable State and Federal laws, executive orders, circulars, directives, regulations, policies, standards, guidelines and operational requirements.

Agencies shall develop processes and mechanisms to:

- (a) Limit personally identifiable information (PII) processed in the information life cycle to the data elements that are required for the business purpose;
- (b) Minimize the use of PII in testing and training systems; and
- (c) In accordance with Media Sanitization requirements, dispose of, destroy, or erase information following the retention period.

Supplemental Guidance: In accordance with the State of New Jersey, Chapter 410, Laws of 1953, [Destruction of Public Records Act](#), the [State General Records Retention Schedule](#), other applicable State and Federal laws, litigation holds, regulations, and agency business requirements, agencies should dispose of information when it is no longer required for the given business purpose in order to reduce security and privacy risks.

## **SI-13: PERSONALLY IDENTIFIABLE INFORMATION**

As appropriate and in accordance with all applicable laws, regulations, executive orders, circulars, directives and policies, agencies shall implement mechanisms and processes to:

- (a) As feasible, collect the PII directly from the individual or their designated representative to help ensure the information is correct;
- (b) Check the accuracy, relevance, timeliness, and completeness of PII across the information life cycle;
- (c) Correct or delete inaccurate or outdated PII;
- (d) Correct or delete PII upon request by individuals or their designated representatives;

- (e) Periodically review and remove information about individuals that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records, and/or information that is linked or linkable to an individual, such as medical, educational, financial, and employment information from datasets when it is no longer required for the given business purpose;
- (f) Remove, mask, encrypt, hash, or replace direct identifiers in a dataset; and
- (g) In accordance with media sanitization requirements, dispose of, destroy, or erase information following the retention period or business purpose has expired.

Supplemental Guidance: Inaccurate PII maintained by agencies may cause problems for individuals, especially in those business functions where inaccurate information may result in inappropriate decisions or the denial of benefits and services to individuals. De-identification is the general term for the process of removing the association between a set of identifying data and the data subject. If a dataset is only used to produce aggregate statistics, the identifiers that are not needed for producing those statistics should be removed. Removing identifiers improves privacy protection since information that is removed cannot be inadvertently disclosed or improperly used. Agencies should dispose of PIII when it is no longer required for the given business purpose in order to reduce security and privacy risks.

## REFERENCES

The requirements established in the System and Information Integrity policies and standards have been derived from the following:

- NIST SP 800-53r5 System and Information Integrity (SI); Media Protection (MP), System and Communications Protection (SC), and Configuration Management (CM), and
- NIST CSF Protect – Data Security (PR.DS), Detect – Security Continuous Monitoring (DE.CM).

---

## SYSTEM AND COMMUNICATIONS PROTECTION (SC)

---

### SC-01: PURPOSE

The purpose of the Systems and Communications Protection policies and standards is to establish baseline administrative, physical, and technical security controls for the protection of State information systems, networks, and the information they store, process, and transmit.

### KEY TERMS

**Boundary Protection Device** - A device with appropriate mechanisms that:

- (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or
- (ii) provides information system boundary protection.

**Proxy Server** - A server that services the requests of its clients by forwarding those requests to other servers.

### SC-02: POLICY

Agencies shall implement administrative, physical, and technical security controls for the protection of State information systems and communications.

#### ENTERPRISE Network Management

Unless otherwise specified by contract or written agreement:

- (a) The New Jersey Office of Information Technology (NJOIT) shall be responsible for procuring, designing, managing, implementing, monitoring, and securing the State of New Jersey Garden State Network (GSN) that provides information technology and telecommunications resources, including WAN aggregation, remote access, data center connectivity, and Internet services to Executive Branch Departments and Agencies;
- (b) Executive Branch Agencies, whether independently or through a service agreement with NJOIT, shall be responsible for the development and implementation of network and telecommunications designs, processes, and technical security controls necessary to provide authorized access to agency technology resources, in accordance with the technical standards defined by NJOIT;
- (c) The NJOIT shall be responsible for the central management and allocation of the IP address space and Domain Name Services (DNS) used to provide network services to GSN entities;
- (d) NJOIT and agencies shall manage networks and their respective information systems in accordance with industry standard practices and to the greatest extent possible require that systems use standard ports and services (e.g. port 80 for HTTP, 443 HTTPS) as defined in the Internet Assigned Numbers Authority [Service Name and Transport Protocol](#)

[Number Registry](#) in order to ensure network interoperability least functionality, and standardization.

- (e) NJOIT shall follow [Request For Comments \(RFC\) 1918](#) for the assignment of private (internal) Internet Protocol addresses

Supplemental Guidance: The objective is to ensure the protection of information in networks and their supporting information processing facilities. Networks should be managed and controlled to protect information in systems and applications.

Consistent with [Executive Order 225](#), the Office of Information Technology is responsible for providing and maintaining the information technology infrastructure (computer, network, and storage) of the Executive Branch, including all ancillary departments and agencies of the Executive Branch. Within this Manual, the policies and standards require agencies to implement safeguards necessary to protect information assets against a loss of confidentiality, integrity, and availability. The term agency includes OIT and all ancillary departments and agencies. Agencies must coordinate all network design, implementation, management, and operations with OIT to ensure security is accounted for throughout the GSN.

### **SC-03: IDENTIFIED RESPONSIBILITY**

Agency CIOs, or their qualified designees, are identified as the final decision makers regarding the management of, changes to, updates to, or modifications of agency owned and/or managed networks and network devices, in accordance with the technical standards defined by NJOIT and the security requirements as defined in this Manual and documented herein, or otherwise required by policy, statute, regulation, or contract.

### **SC-04: SEPARATION OF SYSTEM AND USER FUNCTIONALITY**

Agencies shall implement physical and/or logical controls to separate, user functionality, including user interface services, from system management functionality.

Supplemental Guidance: System management functionality includes functions that are necessary to administer databases, network components, workstations, or servers. These functions typically require privileged user access. Agencies may separate system management functions from user functions by using different computers, instances of operating systems, central processing units, or network addresses; by employing virtualization techniques; or some combination of these or other methods. Separation of system management functions from user functions includes web administrative interfaces that employ separate authentication methods for users of any other system resources. Separation of system and user functions may include isolating administrative interfaces on different domains and with additional access controls. The separation of system and user functionality can be achieved by applying the systems security engineering design principles.

### **SC-05: INFORMATION IN SHARED SYSTEM RESOURCES**

Agency Asset Custodians shall configure systems and implement controls to prevent an unauthorized and/or unintended information transfer via shared system resources.

Supplemental Guidance: Preventing unauthorized and unintended information transfer via shared system resources stops information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system. Information in shared system resources also applies to encrypted representations of information. In other contexts, control of information in shared system resources is referred to as object reuse and residual information protection. Information in shared system resources does not address information remanence, which refers to the residual representation of data that has been nominally deleted; covert channels (including storage and timing channels) where shared system resources are manipulated to violate information flow restrictions; or components within systems for which there are only single users or roles.

## **SC-06: DENIAL-OF-SERVICE PROTECTION**

Agencies shall:

- (a) Plan and configure their networks and systems to limit the effects of denial-of-service attacks; and
- (b) At a minimum, employ the following controls to achieve the denial-of-service objective:
  1. Boundary protection devices (e.g. routers and firewalls) that filter certain types of packets to protect system components on internal networks from being directly affected;
  2. Authentication mechanisms that restrict access to systems and services to only authorized and authenticated users; and
  3. Denial –of-Service monitoring and mitigation systems and services.

Supplemental Guidance: Denial-of-service events may occur due to a variety of internal and external causes, such as an attack by an adversary, or a lack of planning to support agency, or system needs with respect to capacity and bandwidth. Employing increased network capacity and bandwidth combined with service redundancy also reduces the susceptibility to denial-of-service events. The State, through the NJOIT and NJCCIC, implements enterprise controls and services to mitigate the risks of:

- Volumetric Attacks – These attacks operate by sending more connection requests (such as transmission control protocol (TCP) synchronize or SYN messages) than can be processed by the target.
- Application Layer Attacks – A common type of application layer attack uses HTTP GET or HTTP POST requests to overwhelm a web server. HTTP GET requests retrieve static content from web servers, and are easy to craft. HTTP POST requests retrieve more dynamic content, and can be used to tie up processing power or generate large responses.
- Reflection and Amplification Attacks – These attacks target and exploit network protocols such as domain name system (DNS), character generation (CHARGEN) and network time

protocol (NTP). Amplification attacks generate large responses from small requests; and reflection attacks use spoofing to direct unwanted responses to a target IP address.

- **Stealthy Attacks** - These attacks, such as Slowloris, are designed to exhaust the resources of targeted web servers by sending partial HTTP requests at regularly timed intervals to keep connections open as long as possible. Eventually, the open connections will fill the web server's maximum concurrent connection pool, denying additional connection attempts from legitimate users. The result is a stealthy, low bandwidth attack that disables a specific web server in a way that avoids triggering volumetric-based detection mechanisms.

These controls and services are available to all agencies.

## **SC-07: BOUNDARY PROTECTION**

Agencies shall:

- (a) Monitor and control communications at the externally managed interfaces to all systems under their purview and the key internally managed interfaces within the systems;
- (b) Implement subnetworks for publicly accessible system components that are physically and logically separated from internal organizational networks, as appropriate; and
- (c) Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with the State's enterprise security and privacy architecture.

Supplemental Guidance: Boundary protections (e.g. firewalls and routers) are typically implemented as a common control for all or part of an organizational network such that the boundary to be protected is greater than a system-specific boundary (e.g. an authorization boundary). Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization systems, or encrypted tunnels implemented within a security architecture.

Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones (DMZs).

Restricting or prohibiting interfaces within agency systems includes restricting external web traffic to designated web servers within managed interfaces, prohibiting external traffic that appears to be spoofing internal addresses, and prohibiting internal traffic that appears to be spoofing external addresses.

### **SC-07.1: ACCESS POINTS**

All Internet access points that provide connectivity between the GSN and the public Internet shall be procured, implemented, and managed throughout their lifecycle by the NJOIT. Agencies shall ensure the NJOIT is aware of any current or future plans for external network connections. The number of external network connections to the Garden State Network shall be limited and controlled.

Supplemental Guidance: Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic. The Trusted Internet Connection (TIC) initiative is an example of limiting the number of external network connections. For more information, see <https://www.dhs.gov/trusted-internet-connections>.

## **SC-07.2: EXTERNAL TELECOMMUNICATIONS/DATA SERVICES**

Agencies shall:

- (a) Implement a managed interface for each external telecommunication/data service;
- (a) Establish a traffic flow policy for each managed interface;
- (b) Protect the confidentiality and integrity of the information being transmitted across each interface;
- (c) Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;
- (d) Review exceptions to the traffic flow policy annually and remove exceptions that are no longer supported by an explicit mission or business need;
- (e) Prevent unauthorized exchange of control plane traffic with external networks;
- (f) Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and
- (g) Filter unauthorized control plane traffic from external networks.

Supplemental Guidance: External telecommunications/data services can provide data and/or voice communications services. Examples of control plane traffic include Border Gateway Protocol (BGP) routing, Domain Name System (DNS), and management protocols.

## **SC-07.3: DENY BY DEFAULT/ALLOW BY EXCEPTION**

Agencies shall configure managed interfaces to deny network communications traffic by default and allow network communications traffic by exception.

Supplemental Guidance: Denying by default and allowing by exception applies to inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those system connections that are essential and approved are allowed. Deny by default, allow by exception also applies to a system that is connected to an external system.

## **SC-07.4: SPLIT TUNNELING FOR REMOTE DEVICES**

Agencies shall implement controls to prevent split tunneling for remote devices connecting to systems and networks within the GSN unless the split tunnel is necessary for conducting agency business and is securely provisioned.

Supplemental Guidance: Split tunneling is the process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network. This method of network access enables a user to access remote devices and simultaneously, access uncontrolled networks. Split tunneling might be desirable by remote users to communicate with local system resources, such as printers, and even external services, such as websites and cloud-based resources. Agencies may allow for the use of split tunneling, providing that the endpoint from which a remote connection is being made from is configured with appropriate controls and mechanisms (e.g. EDR software, host-based firewall, host-based web-filtering software, etc.)

## **SC-07.5: PROXY SERVERS**

Agencies shall:

- (a) Prohibit direct public access between the Internet and any system on their internal networks. Route traffic through authenticated proxy servers as approved by NJOIT;
- (b) Develop and implement network-based URL filters that limit a system's ability to connect to prohibited websites, based on content and/or reputation;
- (c) Develop policies that document permitted and prohibited web content categories for agency personnel;
- (d) Prohibit access to website content that is prohibited by State or Federal law, and State or agency policies;
- (e) Authorize and manage exceptions and exemptions to the prohibited web content categories as appropriate for agency personnel based on their roles and responsibilities; and
- (f) Enforce filtering for all systems, whether the system is physically located within State facilities or not.

Supplemental Guidance: External networks as referred to above are considered networks outside of NJOIT or agency control. A proxy server is a server (e.g. system or application) that acts as an intermediary for clients requesting system resources from external systems and services. System resources that may be requested include files, connections, web pages, or services.

Web content filtering devices are one of the most common proxy servers that provide access to the Internet. Proxy servers can support the logging of Transmission Control Protocol (TCP) sessions and the blocking of specific Uniform Resource Locators (URLs), Internet Protocol (IP) addresses, and domain names. Web proxies can be configured with agency-defined lists of authorized and unauthorized websites.

## **SC-07.6: PREVENT EXFILTRATION/DATA LOSS PREVENTION**

As technically feasible, agencies shall implement Data Loss Prevention (DLP) technologies that monitor and prevent the unauthorized transfer of sensitive information including, but not

limited to, personally identifiable information (PII) from agency systems and services to external networks.

All agency email systems are required to use the NJCCIC's enterprise email filtering solution to monitor and prevent PII from being sent to external entities without approved safeguards (e.g. encryption) to protect confidentiality and privacy.

Supplemental Guidance: Managing the processing of PII is an important aspect of protecting an individual's privacy. Applying, monitoring for, and documenting exceptions to processing rules ensures that PII is processed only in accordance with established privacy requirements. Proxy servers, web- and email-filtering technologies, secure file transfer technologies, as well as host-based DLP and EDR software are some of the mechanisms that agencies may use to prevent exfiltration of sensitive data. Beyond technical solutions, users should use due care when collecting, processing, and transmitting PII, including ensuring emails are addressed to the correct recipients.

### **SC-07.7: HOST BASED PROTECTION**

As technically and operationally feasible, agencies shall implement host-based boundary protection mechanisms such as host-based firewalls on all agency servers, workstations, notebook computers, and mobile devices.

### **SC-08: TRANSMISSION CONFIDENTIALITY AND INTEGRITY**

Agencies shall implement physical and logical controls and processes to protect the confidentiality, integrity, and privacy of transmitted information.

Supplemental Guidance: Physical controls and processes include securing of network devices, interfaces, and cabling from unauthorized physical access. Logical controls include, but are not limited to, implementing FIPS 140-2 compliant cryptographic mechanisms (e.g. TLS and IPsec) to prevent the unauthorized disclosure or changes to information during transmission. Cryptographic mechanisms used to protect information integrity include cryptographic hash functions that have applications in digital signatures, checksums, and message authentication codes.

### **SC-09: NETWORK DISCONNECT**

Asset Custodians shall configure systems:

- (a) To terminate the network connection associated after a 30-minute period of inactivity, such that the user must re-authenticate to resume or establish a new session; and
- (b) Limit remote access sessions to a period of no more than 24 consecutive hours without requiring the user to re-authenticate.

Supplemental Guidance: Terminating network connections associated with specific communications sessions includes de-allocating TCP/IP address or port pairs at the operating system level and de-allocating the networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. The baseline

time periods for this control are 30 minutes and 24 consecutive hours. Agencies may adjust these baselines in individual circumstances based on business and operational needs. Adjustments are required to be documented, monitored, and periodically evaluated.

## **SC-10: CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT**

Agencies shall establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements:

- (a) Use FIPS 140-2 compliant encryption mechanisms (a list of products and modules validated by NIST can be found at the [NIST Cryptographic Management Verification Program \(CMVP\) website](#));
- (b) Maintain availability of information in the event of the loss of cryptographic keys by users;
- (c) Control access to and distribution of cryptographic keys including the following requirements;
  - 1. Change cryptographic keys that have reached the end of their cryptoperiod;
  - 2. Retire or replace (e.g., archive, destroy and/or revoke) keys as deemed necessary when the integrity of the key has been weakened (e.g., departure of an employee with knowledge of a clear-text key), or keys are suspected of being compromised;
  - 3. Only use archived cryptographic keys for decryption/verification purposes;
  - 4. Enforce split knowledge and dual control if manual, clear-text cryptographic key management operations are used;
  - 5. Prevent the unauthorized substitution of cryptographic keys;
  - 6. Require cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities;
  - 7. Store keys securely (separate from data) and make readily available, if needed, for later decryption; and
- (d) Use only digital certificates either issued by and/or approved by the NJOIT for publicly accessible systems, applications, and networks.

Supplemental Guidance: Products and modules that have been validated by NIST as FIPS 140-2 compliant can be found at the [NIST Cryptographic Management Verification Program \(CMVP\) website](#). Agencies that require certificates for agency information systems should contact the NJOIT and/or the NJCCIC to ensure only approved certificate management authorities are used.

## **SC-11: CRYPTOGRAPHIC PROTECTION**

Agencies shall ensure strong cryptography (FIPS 140-2) is used to protect data at rest, in transit, and in use in accordance with applicable State and Federal statutes, regulatory requirements, circulars, directives, policies, contractual obligations, and other agency-defined confidentiality and integrity concerns.

## SC-11.1: DATA AT REST

Agencies shall:

- (a) Employ full-disk encryption for all agency laptop and notebook computers;
- (b) Employ full-disk encryption for all agency desktop computers, workstations, and servers that are used outside of agency-controlled locations (e.g. employee homes);
- (c) Implement mechanisms to encrypt sensitive data on other mobile computing devices and portable computing devices, such as smart phones, tablets and portable storage devices (such as compact disks (CDs), digital video disks (DVDs), and flash drives) that are used to conduct State business;
- (d) Employ field-level encryption to protect data in shared databases and stores in which multiple people with varying access approval levels; and
- (e) Conduct a risk analysis of other stored sensitive information to determine the need for the employment of encryption to protect its confidentiality and integrity.

## SC-11.2: DATA IN TRANSIT

Agencies shall employ strong encryption and current versions of security protocols (e.g. TLS, IPSEC, SSH) to protect the confidentiality and integrity of information in transit.

Supplemental Guidance: Agencies should refer to NIST Special Publication (SP) 800-52 Revision 2, [Guidelines for the Selection, Configuration, and Use of Transport Layer Security \(TLS\) Implementations](#) for additional guidance on the use of cryptographic protocols to be used to protect data in transit.

## SC-11.3: PUBLICLY ACCESSIBLE WEBSITE AND SERVICES

Agencies shall ensure that all publicly accessible State of New Jersey Executive Branch Government websites and web services provide secure and private connections through the use of an HTTPS connection.

- (a) Newly developed websites and services at all New Jersey State agency domains or subdomains must adhere to this policy upon launch; and
- (b) For existing websites and services, agencies should prioritize deployment using a risk-based analysis. Web services that involve an exchange of personally identifiable information (PII), or where the content is unambiguously sensitive in nature, or where the content receives a high-level of traffic, should receive priority and migrate as soon as possible.

Supplemental Guidance: Various State and Federal statutes and regulations require the encryption of sensitive information including, but not limited to, Federal Tax Information (FTI), medical records, payment card information, Criminal Justice Information (CJI), etc. Agencies should review the data types they use to ensure compliance with all applicable laws and regulations regarding cryptographic protection obligations. Agencies should refer

to NIST Special Publication (SP) 800-175B [Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms](#) for guidance on the selection and implementation of cryptographic controls based on the security categorization and risk environment of the data and/or information system.

## **SC-12: COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS**

Agencies shall prohibit remote activation of collaborative computing devices without providing an explicit indication of use to users physically present at the devices.

Supplemental Guidance: Collaborative computing devices and applications include remote meeting and video teleconference devices and applications, networked white boards, cameras, and microphones. The explicit indication of use includes signals to users when collaborative computing devices and applications are activated.

## **SC-13: PUBLIC KEY INFRASTRUCTURE CERTIFICATES**

Agencies shall coordinate the issuance of public key infrastructure certificates or otherwise obtain public key certificates from an NJOIT approved certificate authority/service provider.

Supplemental Guidance: Public key infrastructure (PKI) certificates are certificates with visibility external to agency systems and certificates related to the internal operations of systems, such as application-specific time services. Public key certificates must be issued by using a secure process that both verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party.

## **SC-14: MOBILE CODE**

Agencies shall:

- (a) Define acceptable and unacceptable mobile code and mobile code technologies; and
- (b) Authorize, monitor, and control the use of mobile code within the system.

Supplemental Guidance: Mobile code includes any program, application, or content that can be transmitted across a network (e.g., embedded in an email, document, or website) and executed on a remote system. Decisions regarding the use of mobile code within agency systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include Java applets, JavaScript, HTML5, WebGL, VBScript, batch files, etc. Usage restrictions and implementation guidelines apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices, including notebook computers and smart phones. Mobile code control strategies include web- and email -filtering technologies to prevent the download of mobile code and mobile code technologies, endpoint detection and response software that blocks mobile code and mobile code technologies from executing, etc.

## **SC-15: SECURE NAME/ADDRESS RESOLUTION SERVICE**

NJOIT and agencies authorized by NJOIT to provide Domain Name Services shall:

- (a) Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries;
- (b) Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace; and
- (c) Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Supplemental Guidance: Providing authoritative source information enables external clients, including remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service.

Systems that provide name and address resolution services include domain name system (DNS) servers. Additional artifacts include DNS Security Extensions (DNSSEC) digital signatures and cryptographic keys. Authoritative data includes DNS resource records. The means for indicating the security status of child zones includes the use of delegation signer resource records in the DNS. Systems that use technologies other than DNS to map between host and service names and network addresses are to provide other means to assure the authenticity and integrity of response data. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Systems that use technologies other than DNS to map between host and service names and network addresses are to provide some other means to enable clients to verify the authenticity and integrity of response data.

## **SC-16: ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE**

NJOIT is responsible for the management of the State's enterprise Domain Name Services. NJOIT and/or agencies to whom NJOIT has delegate authority to manage DNS shall:

- (a) Ensure the systems that collectively provide name/address resolution service for the State or an agency are fault-tolerant and implement internal and external role separation.
- (b) Maintain at least two (2) authoritative domain name system (DNS) servers to eliminate single points of failure and to enhance redundancy. One should be configured as the primary server and the other configured as the secondary server.
- (c) Ensure servers are deployed in two (2) geographically separated network physical locations and subnetworks.
- (d) Configure the servers to provide redundancy, load balancing, and distributed access.
- (e) Configure DNS servers with internal roles to only process name and address resolution requests from within the Garden State Network and use recursive or

cached name resolution.

- (f) Configure DNS servers with external roles to only process name and address resolution information requests from clients external to the GSN.

## **SC-17: SESSION AUTHENTICITY**

Agencies shall:

- (a) Implement protection mechanisms to ensure adequate protection of data integrity, confidentiality, and authenticity in communications sessions. Mechanisms include, but are not limited to, the following:
- Security services based on IPsec
  - VPNs
  - TLS
  - DNS
  - SSH
  - Digital signatures
  - Digital certificates
  - Digital time stamping
  - FIPS 140-2 approved encryption technology
- (b) Ensure the information system invalidates session identifiers upon user logout or other session termination to curtail the ability of adversaries from capturing and continuing to employ previously valid session IDs; and
- (c) Configure the information system to generate a unique session identifier for each session and recognize only session identifiers that are system-generated.

Supplemental Guidance: Protecting session authenticity addresses communications protection at the session level, not at the packet level. Such protection establishes grounds for confidence at both ends of communications sessions in the ongoing identities of other parties and the validity of transmitted information. Authenticity protection includes protecting against “man-in-the-middle” attacks, session hijacking, and the insertion of false information into sessions. Invalidating session identifiers at logout curtails the ability of adversaries to capture and continue to employ previously valid session IDs. Generating unique session identifiers curtails the ability of adversaries to reuse previously valid session IDs. Employing the concept of randomness in the generation of unique session identifiers protects against brute-force attacks to determine future session identifiers.

## **SC-18: PROCESS ISOLATION**

Agencies shall maintain a separate execution domain for each executing system process.

Supplemental Guidance: Systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. Process isolation technologies, including sandboxing or virtualization, logically separate software and firmware from other software, firmware, and data. Process isolation helps limit the access of potentially untrusted software to other system resources. The capability to maintain separate execution domains is available in commercial operating systems that employ multi-state processor technologies.

## **SC-19: USAGE RESTRICTIONS**

Agencies shall:

- (a) Establish usage restrictions and implementation guidelines for hardware, software, or firmware components (e.g., open-source software, SaaS applications, mobile devices, portable storage devices, VOIP, mobile code, digital copiers, printers, scanners, wireless technologies, mobile devices); and
- (b) Authorize, monitor, and control the use of such components within the system.

Supplemental Guidance: Usage restrictions apply to all system components including, but not limited to mobile code, mobile devices, wireless access, and wired and wireless peripheral components (e.g., copiers, printers, scanners, optical devices, and other similar technologies). The usage restrictions and implementation guidelines are based on the potential for system components to cause damage to the system and help to ensure that only authorized system use occurs.

Agencies are to refer to the mobile device management requirements for applicable usage restrictions related to mobile devices.

## **SC-20: DETONATION CHAMBERS**

As technically and operationally feasible, agencies tasked with conducting incident response and forensics shall employ a detonation chamber in a secure, quarantined environment to perform the following:

- (a) Allow the opening of email attachments;
- (b) Allow the execution of untrusted or suspicious applications;
- (c) Allow the execution of Universal Resource Locator (URL) requests in the safety of an isolated environment or virtualized sandbox to quickly identify malicious code; and

(d) Prevent the propagation of malicious code to user and production environments.

Supplemental Guidance: Detonation chambers, also known as dynamic execution environments, allow agencies to open email attachments, execute untrusted or suspicious applications, and execute Universal Resource Locator (URL) requests in the safety of an isolated environment or a virtualized sandbox. Protected and isolated execution environments provide a means of determining whether the associated attachments or applications contain malicious code. While related to the concept of deception nets, the employment of detonation chambers is not intended to maintain a long-term environment in which adversaries can operate and their actions can be observed.

## **REFERENCES**

The requirements established in the Systems and Communications Protection policies and standards have been derived from following:

NIST SP 800-53r5 Systems and Communication Protection (SC), Access Control (AC); Security Assessment and Authorization (CA); and

NIST CSF Protect/Access Control (PR-AC). Protect/Protective Technologies (PR-PT).

---

## SYSTEM AND SERVICES ACQUISITION (SA)

---

### SA-01: PURPOSE

The purpose of System and Services Acquisition policies and standards is to establish the minimum requirements necessary to ensure that systems and services developed or acquired by State of New Jersey Executive Branch Departments and Agencies perform as intended to maintain information confidentiality, integrity, availability, and privacy.

### KEY TERMS

**Center for Internet Security (CIS) Benchmarks** - CIS benchmarks are configuration baselines and best practices for securely configuring a system.

**Information System Service** - A capability provided by an information system that facilitates information processing, storage, or transmission.

**Software Development Life Cycle (SDLC)** – The scope of activities associated with the development of a software application that includes planning, analysis, design, testing, and implementation. The acronym, SDLC is interchangeably used to refer to System Development Life Cycle which includes the same scope of activities of a Software Development Life Cycle.

**Major Applications and Systems** – A major application or system is described as any system or application that includes one or more of the following characteristics:

- (a) Includes users in more than one agency;
- (b) Costs more than \$200,000 to develop and implement (cost includes hardware, software, and contract personnel);
- (c) Any public-facing web application; and/or
- (d) Any application that stores or processes sensitive information or is deemed critical to the operations of the agency.

**Personal Identity Verification** - A physical artifact (e.g., identity card, “smart” card) issued to a government individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable). PIV requirements are defined in [FIPS PUB 201-2](#).

**Sensitive Information** - A term to describe any information which requires protection from unauthorized access or disclosure.

### SA-02: POLICY

Agencies shall ensure security and privacy processes and controls are planned for and implemented throughout the lifecycles of all systems and services they develop or acquire.

## **SA-03: ALLOCATION OF RESOURCES**

Agencies shall:

- (a) Determine the high-level information security and privacy requirements for the system or system service during the planning phase;
- (b) Determine, document, and allocate the resources required to protect the system or system service as part of the agency's budget planning and investment control process; and
- (c) Establish a discrete line item for information security and privacy in agency programming and budgeting documentation.

Supplemental Guidance: Resource allocation for information security and privacy includes funding for system and services acquisition, sustainment, and supply chain-related risks throughout the system development life cycle.

## **SA-04: SYSTEM DEVELOPMENT LIFE CYCLE**

Agencies shall:

- (a) Acquire, develop, and manage the system using generally accepted system development life cycle processes and phases, such as implementation/planning, analysis/design, acquisition/development, implementation, operations, maintenance, and disposal;
- (b) Define and document information security and privacy roles and responsibilities throughout the system development life cycle;
- (c) Identify individuals having information security and privacy roles and responsibilities;
- (d) Integrate information security and privacy risk management processes into system development life cycle activities;
- (e) Ensure security and privacy protections, commensurate with risks, are implemented in the preproduction (e.g. dev, test, integration, staging), and production environments;
- (f) Approve, document, and control the use of live or operational data, especially sensitive information, in preproduction environments;
- (g) Protect preproduction environments for the system, system component, or system service at the same impact or classification level as any live data in use within the preproduction environments; and
- (h) Plan for and implement a technology refresh schedule for the system throughout the system development life cycle.

Supplemental Guidance: The integration of security and privacy considerations early in the system development life cycle is a foundational principle of systems security engineering and privacy engineering. To apply the required controls within the system development life cycle requires a basic understanding of information security and privacy, threats, vulnerabilities, adverse impacts, and risks to critical mission and business functions.

The use of live or operational data in preproduction environments can result in significant risks. In addition, the use of personally identifiable information in testing, research, and training increases the risk of unauthorized disclosure or misuse of such information. Therefore, it is important for agencies to manage any additional risks that may result from the use of live or operational data. Agencies can minimize such risks by using test or dummy data during the design, development, and testing of systems, system components, and system services.

## **SA-05: ACQUISITION PROCESS**

Agencies procuring information technology equipment and services (e.g. computers, hardware components, software, and cloud services) shall:

- (a) Adhere to all applicable State and Federal procurement laws, executive orders, circulars, directives, regulations, and policies;
- (b) Complete and submit required [System Architecture Review \(SAR\)](#) policy documents to the NJOIT;
- (c) Ensure all vendors and other third parties that:
  - 1. Develop, implement, provide, manage, or host State of New Jersey major systems and applications;
  - 2. Develop, implement, provide, manage, or host State of New Jersey general support systems; and/or
  - 3. Have authorized access to State systems production environments, internal networks, and/or sensitive informationcomplete and submit the Third-Party Information Security Questionnaire to the New Jersey Cybersecurity and Communications Cell (NJCCIC) at [riskreview@cyber.nj.gov](mailto:riskreview@cyber.nj.gov);
- (d) Include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract statement of work, or other applicable agreement vehicle for the system, system component, or service, as applicable:
  - 1. Security and privacy functional requirements;
  - 2. Strength of mechanism requirements;
  - 3. Security and privacy assurance requirements;
  - 4. Controls needed to satisfy the security and privacy requirements;
  - 5. Security and privacy documentation requirements;
  - 6. Requirements for protecting security and privacy documentation;
  - 7. Description of the system development environment and environment in which the system is intended to operate;
  - 8. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and

9. Acceptance criteria.

- (e) Require developer(s) of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented;
- (f) Require developer(s) of an information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes security-relevant external system interfaces, high-level design, source code, or hardware schematics;
- (g) Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use;
- (h) Ensure the intended ports, protocols, and services comply with network management standards as contained herein;
- (i) Include organizational data ownership requirements in the acquisition contract;
- (j) Require all data to be removed from the contractor's system and returned to the agency within a defined time frame;
- (k) Require the developer of the system, system component, or system service to produce a plan for continuous monitoring of control effectiveness that is consistent with the agency's and NJCCIC's continuous monitoring requirements as documented in this Manual;
- (l) Limit the use of commercially provided information assurance and information assurance-enabled information technology products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved [Protection Profile](#) for a specific technology type, if such a profile exists;
- (m) Require, if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that the cryptographic module is FIPS-validated or NSA-approved;
- (n) Employ only information technology products on the [FIPS 201-approved products](#) list for Personal Identity Verification (PIV) capability implemented within organizational systems;
- (o) Require the developer of the system, system component, or system service to deliver the system, component, or service with a configuration (e.g. [CIS Security Benchmark](#)) as required in the Configuration Management section of this Manual; and
- (p) Require the developer of the system, system component, or system service to use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.

Supplemental Guidance: Agencies should contact the Office of Information Technology and/or the Department of Treasury Division of Purchase and Property for guidance regarding applicable State and Federal laws, executive orders, circulars, regulations, and policies governing the procurement of IT equipment and services. Agencies should review the requirements in

[Department of Treasury Joint Circular No. 21-08 OMB/DPP/OIT](#) regarding procurements of information technology (IT) hardware, software, subscription-based solutions and related services and non-IT equipment.

The Third-Party Information Security Questionnaire can be obtained from the NJCCIC at [riskreview@cyber.nj.gov](mailto:riskreview@cyber.nj.gov). The Questionnaire is intended to inform the State as to the degree to which the vendor/third party conforms to the State's information security requirements. In some cases, the State may require additional clarifying information, documentation, and copies of certifications and attestations beyond what was initially provided by the submitting organization. A submission shall not be considered complete until the NJCCIC receives all necessary documentation and completes a Third-Party Information Security Risk Assessment Report.

Based on the overall risk rating as determined by the NJCCIC, the sponsoring agency in consultation with the NJCCIC and NJOIT will determine if the risk rating is acceptable to proceed for the given engagement. Based on the criticality and/or sensitivity of the information system and information in scope, as well as the legal, regulatory, and/or contractual requirements, the State may require the submitting organization to implement additional risk mitigation controls prior to the award of any contract or agreement.

Security and privacy functional requirements are typically derived from the high-level security and privacy requirements described during the planning phase of the SDLC. Functional properties of security and privacy controls describe the functionality (i.e., security or privacy capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls. Agencies may require different levels of detail in the documentation for the design and implementation of controls in agency systems, system components, or system services based on mission and business requirements, requirements for resiliency and trustworthiness, and requirements for analysis and testing.

## **SA-06: SYSTEM DOCUMENTATION**

Agencies shall:

- (a) Obtain or develop administrator documentation for the system, system component, or system service that describes:
  1. Secure configuration, installation, and operation of the system, component, or service;
  2. Effective use and maintenance of security and privacy functions and mechanisms; and
  3. Known vulnerabilities regarding configuration and use of administrative or privileged functions.
- (b) Obtain or develop user documentation for the system, system component, or system service that describes:
  1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;

2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and
  3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals.
- (c) Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent. In such cases, agencies should recreate the necessary documentation to maintain and operate the system securely; and
- (d) As appropriate, distribute documentation to system owners, system security officers, system administrators, and other key stakeholders.

Supplemental Guidance: System documentation helps personnel understand the implementation and operation of controls. System documentation may be used to support the management of supply chain risk, incident response, and other functions. Attempts to obtain documentation include contacting manufacturers or suppliers and conducting web-based searches. The inability to obtain documentation may occur due to the age of the system or component or the lack of support from developers and contractors. When documentation cannot be obtained, agencies may need to recreate the documentation if it is essential to the implementation or operation of the controls. The protection provided for the documentation is commensurate with the security category or classification of the system.

## **SA-07: SECURITY AND PRIVACY ENGINEERING PRINCIPLES**

Agencies shall apply systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components:

Security and privacy engineering principles include:

- (a) Developing layered protections (defense-in-depth);
- (b) Establishing security and privacy policies, architecture, and controls as the foundation for design and development;
- (c) Incorporating security and privacy requirements into the system development life cycle;
- (d) Delineating physical and logical security boundaries, ensuring that developers are trained on how to build secure software;
- (e) Tailoring controls to meet organizational needs; and
- (f) Performing threat modeling to identify use cases, threat agents, attack vectors and patterns, design patterns, and compensating controls needed to mitigate risk.

Supplemental Guidance: Agencies can apply systems security and privacy engineering principles to new systems under development or to systems undergoing upgrades. For existing systems, agencies apply systems security and privacy engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware components within those systems. System security engineering principles can also be used to

protect against certain supply chain risks, including incorporating tamper-resistant hardware into the design.

## **SA-08: EXTERNAL SYSTEM SERVICES**

Agencies shall:

- (a) Require that providers of external system services comply with security and privacy requirements and employ the controls that are at least commensurate with those required in this Manual (NIST SP800—53r5 Moderate Level);
- (b) Define and document oversight and user roles and responsibilities with regard to external system services;
- (c) Monitor control compliance by external service providers on an ongoing basis;
- (d) Conduct an assessment of risk prior to the acquisition or outsourcing of information security services (see Third-Party Information Security Questionnaire requirement above);
- (e) Require providers of the external system services to identify the functions, ports, protocols, and other services required for the use of such services.
- (f) Require external services providers to restrict all agency information storage and processing operations to facilities within the United States; and
- (g) Verify that the acquisition or outsourcing of dedicated information security services is approved by the State Chief Information Security Officer.

Supplemental Guidance: External system services are provided by an external provider, and the agency has no direct control over the implementation of the required controls or the assessment of control effectiveness. External system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define the expectations of performance for implemented controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance.

All information processing and storage of agency data is to be restricted to facilities in the United States to the greatest extent possible in order to facilitate incident response activities, including forensic analyses and investigations, that may be adversely affected by the governing laws, policies, or protocols in locations outside of the US.

## **SA-09: DEVELOPER CONFIGURATION MANAGEMENT**

Agencies shall require the developer of the system, system component, or system service to:

- (a) Perform configuration management during system, component, or service design, development, implementation, operation, and disposal of:
  - 1. Internal system development and system integration of commercial software; and
  - 2. External system development and system integration.

- (b) Document, manage, and control the integrity of changes to configuration items under configuration management;
- (c) Implement only agency-approved changes to the system, component, or service;
- (d) Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and
- (e) Track security flaws and flaw resolution within the system, component, or service.

Supplemental Guidance: Agencies should consider the quality and completeness of configuration management activities conducted by developers as direct evidence of applying effective security controls. Controls include protecting the master copies of material used to generate security-relevant portions of the system hardware, software, and firmware from unauthorized modification or destruction. Maintaining the integrity of changes to the system, system component, or system service requires strict configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes.

The configuration items that are placed under configuration management include the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the current running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and source code with previous versions; and test fixtures and documentation. Depending on the mission and business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance stage of the system development life cycle.

## **SA-10: DEVELOPER TESTING AND EVALUATION**

Agencies shall:

- (a) Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle to:
  - 1. Develop and implement a plan for ongoing security and privacy control assessments;
  - 2. Perform unit; integration; system; and regression testing/evaluation as appropriate throughout the life cycle of the system;
  - 3. Employ static and dynamic code analysis tools to identify common flaws and document the results of the analysis;
  - 4. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;
  - 5. Implement a verifiable flaw remediation process; and
  - 6. Correct flaws identified during testing and evaluation.
- (b) Require the developer of the system, system component, or system service to perform vulnerability testing during development and the subsequent testing, evaluation, and

remediation of moderate, high, and critical vulnerabilities prior to implementation in the production environment;

- (c) Verify the correct implementation of the developer security and privacy assessment plans and the evidence produced during testing and evaluation;
- (d) As applicable by State or Federal laws, regulation, circulars, directives, and policies, and/or commensurate with the criticality and sensitivity of the system, require an independent agent to verify the correct implementation of the developer security and privacy assessment plans and the evidence produced during testing and evaluation;
- (e) Verify that the independent agent is provided with sufficient information to complete the verification process or is granted the authority to obtain such information; and
- (f) Ensure controls that have been determined to be either absent or not operating as intended during security testing/evaluation be remediated prior to implementation in the production environment.

Supplemental Guidance: Developmental testing and evaluation confirms that the required controls are implemented correctly, operating as intended, enforcing the desired security and privacy policies, and meeting established security and privacy requirements. Security properties of systems and the privacy of individuals may be affected by the interconnection of system components or changes to those components. Ongoing assessment during development allows for additional types of testing and evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as manual code review, security architecture review, and penetration testing, as well as static analysis, dynamic analysis, binary analysis, or a hybrid of the three analysis approaches.

Developers can use the analysis approaches, along with security instrumentation and fuzzing, in a variety of tools and in source code reviews. The security and privacy assessment plans include the specific activities that developers plan to carry out, including the types of analyses, testing, evaluation, and reviews of software and firmware components; the degree of rigor to be applied; the frequency of the ongoing testing and evaluation; and the types of artifacts produced during those processes. The depth of testing and evaluation refers to the rigor and level of detail associated with the assessment process. The coverage of testing and evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security and privacy assessment plans, flaw remediation processes, and the evidence that the plans and processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the system. Contracts may specify protection requirements for documentation.

## **SA-11: DEVELOPMENT PROCESS, STANDARDS, AND TOOLS**

Agencies shall:

- (a) Require the developer of the system, system component, or system service to follow a documented development process that:

1. Explicitly addresses security and privacy requirements;
  2. Identifies the standards and tools used in the development process;
  3. Documents the specific tool options and tool configurations used in the development process; and
  4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development.
- (b) Require the developer of the system, system component, or system service to perform a criticality analysis with a level of rigor commensurate with the sensitivity and criticality of the system, system component; and system service at the outset of the SDLC and prior to any subsequent changes, modifications, or upgrades; and
- (c) Review the development process, standards, tools, tool options, and tool configurations to determine if the process, standards, tools, tool options, and tool configurations selected and employed can satisfy the necessary security and privacy requirements.

Supplemental Guidance: Development tools include programming languages and computer-aided design systems. Reviews of development processes include the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes facilitates effective supply chain risk assessment and mitigation. Such integrity requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes.

Criticality analysis performed by the developer provides input to the criticality analysis performed by agencies. Developer input is essential to criticality analysis because agencies may not have access to detailed design documentation for system components that are developed as commercial off-the-shelf products. Such design documentation includes functional specifications, high-level designs, low-level designs, source code, and hardware schematics.

## **SA-12: DEVELOPER-PROVIDED TRAINING**

Agencies shall require the developer of the system, system component, or system service to provide training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms.

Supplemental Guidance: Developer-provided training applies to external and internal (in-house) developers. Training personnel is essential to ensuring the effectiveness of the controls implemented within organizational systems. Types of training include web-based and computer-based training, classroom-style training, and hands-on training (including micro-training). Agencies can also request training materials from developers to conduct in-house training or offer self-training to agency personnel. Agencies are to determine the type of training necessary and may require different types of training for different security and privacy functions, controls, and mechanisms.

## **SA-13: DEVELOPER SCREENING**

Agencies shall require that the developer of the system, system component, or system service:

- (a) Has appropriate access authorizations as determined by the agency; and
- (b) Satisfies the personnel screening criteria consistent with all applicable State and Federal laws, executive orders, regulations, circulars, directives, policies, and guidelines .

Supplemental Guidance: Developer screening is directed at external developers. Because the system, system component, or system service may be used in critical activities essential to the security interests of the State of New Jersey, agencies should have a strong interest in ensuring that developers are trustworthy. The degree of trust required of developers may need to be consistent with that of the individuals who access the systems, system components, or system services once deployed. Authorization and personnel screening criteria include clearances, background checks, citizenship, and nationality. Developer trustworthiness may also include a review and analysis of company ownership and relationships that the company has with entities that may potentially affect the quality and reliability of the systems, components, or services being developed. Satisfying the required access authorizations and personnel screening criteria includes providing a list of all individuals who are authorized to perform development activities on the selected system, system component, or system service so that organizations can validate that the developer has satisfied the authorization and screening requirements.

## **SA-14: UNSUPPORTED SYSTEM COMPONENTS**

Agencies shall:

- (a) Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or
- (b) Isolate or otherwise prohibit the connection of unsupported system components to public or uncontrolled networks.

Supplemental Guidance: Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts. An example of unsupported components includes when vendors no longer provide critical software patches or product updates, which can result in an opportunity for adversaries to exploit weaknesses in the installed components.

Exceptions to replacing unsupported system components include systems that provide critical mission or business capabilities where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option.

Alternative sources for support address the need to provide continued support for system components that are no longer supported by the original manufacturers, developers, or vendors when such components remain essential to agency mission and business functions

## REFERENCES

The requirements established in the System and Services Acquisition policies and standards have been derived from the following references:

NIST SP 800-53r5: Planning (PL), System and Services Acquisition (SA); Assessment, Authorization, and Monitoring (CA); System and Information Integrity (SI); System and Communication Protection (SC); Security Awareness Training (AT);

NIST CSF: Protect/Data Security (PR.DS); Protect/Awareness and Training (PR.AT); and  
CIS Security Benchmarks.

---

## SUPPLY CHAIN RISK MANAGEMENT (SU)

---

### SU-01: PURPOSE

The purpose of the Supply Chain Risk Management policies and standards is to ensure that supply chain risks are appropriately identified, assessed, and managed in order to limit harm or consequences from supply chain-related events.

### KEY TERMS

**Component** - A discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents a building block of an information system. Information system components include commercial information technology products. Also referred to as a system component.

**Due Diligence** - The requirement that organizations must develop and deploy a protection plan to prevent fraud, abuse, and additional deploy a means to detect them if they occur.

**Supplier** – An organization or individual that enters into an agreement with the acquirer or integrator for the supply of a product or service. This includes all suppliers in the supply chain. Includes (i) developers or manufacturers of information systems, system components, or information system services; (ii) vendors; and (iii) product resellers.

**Supply Chain** - A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers.

**Third Party** - Any entity that an agency does business with. This may include suppliers, vendors, contractor, business partners, and other organizations.

### SU-02: POLICY

Agencies shall employ processes and procedures to protect against supply chain risks to systems, system components, or system services and to limit the harm or consequences from supply chain-related events.

Supplemental Guidance: Information systems (including system components that compose those systems) need to be protected throughout the system development life cycle (i.e., during design, development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement).

### SU-03: SUPPLY CHAIN RISK MANAGEMENT PLAN

The dependence on products, systems, and services from external providers, as well as the nature of the relationships with those providers, present an increasing level of risk to the State. Threat actions that may increase security or privacy risks include unauthorized production, the insertion or use of counterfeits, tampering, theft, insertion of malicious software and hardware, and poor manufacturing and development practices in the supply chain. Supply chain risks can be endemic

or systemic within a system element or component, a system, an organization, a sector, or the Nation.

Agencies shall:

- (a) Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of agency systems, system components or system services;
- (b) Review and update the supply chain risk management plan as required, to address threat, organizational, or environmental changes;
- (c) Protect the supply chain risk management plan from unauthorized disclosure and modification; and
- (d) Establish a supply chain risk management team consisting of information technology, security, privacy, legal, and procurement personnel who lead and support acquisition and procurement activities.

Supplemental Guidance: Managing supply chain risk is a complex, multifaceted undertaking that requires a coordinated effort across all agencies to build trust relationships and communicate with internal and external stakeholders. Supply chain risk management (SCRM) activities include identifying and assessing risks, determining appropriate risk response actions, developing SCRM plans to document response actions, and monitoring performance against plans. The SCRM plan (at the system-level) is implementation specific, providing policy implementation, requirements, constraints, and implications.

## **SU-04: SUPPLY CHAIN CONTROLS AND PROCESSES**

Agencies shall:

- (a) Establish processes and procedures to identify and address weaknesses or deficiencies in the supply chain elements including:
  - 1. Hardware, software, and firmware development processes;
  - 2. Shipping and handling procedures;
  - 3. Personnel security and physical security programs;
  - 4. Configuration management tools, techniques, and measures to maintain provenance; and/or
  - 5. Other programs, processes, or procedures associated with the development, acquisition, maintenance and disposal of systems and system components.
- (b) Employ controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events; and
- (c) Document the selected and implemented supply chain processes and controls.

Supplemental Guidance: Supply chain elements include agencies, entities, or tools employed for the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of systems and system components. Supply chain elements and processes may be provided by organizations, system integrators, or external providers. Weaknesses or deficiencies in supply chain elements or processes represent potential vulnerabilities that can be exploited by adversaries to cause harm to the organization and affect its ability to carry out its core missions or business functions.

## **SU-05: ACQUISITION STRATEGIES, TOOLS, AND METHODS**

Agencies shall employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks.

- (a) Adhering to all State and Federal laws, executive orders, circulars, policies, and guidelines pertaining to procurements of systems, system components, and/or services;
- (b) Obscuring the end use of a system or system component;
- (c) Using blind or filtered buys;
- (d) Requiring tamper-evident packaging; or
- (e) Using trusted or controlled distribution.

Supplemental Guidance: Agencies should contact the Office of Information Technology and/or the Department of Treasury Division of Purchase and Property for guidance regarding applicable State and Federal laws, executive orders, circulars, directives, regulations, policies, and guidelines governing the procurement of systems, system components, and services.

Tools and techniques may provide protections against unauthorized production, theft, tampering, insertion of counterfeits, insertion of malicious software or backdoors, and poor development practices throughout the system development life cycle.

## **SU-06: SUPPLIER ASSESSMENTS AND REVIEWS**

Agencies shall assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide:

- (a) Prior to contracting with a supplier;
- (b) At least annually thereafter;
- (c) In response to a supply chain incident involving the supplier; and/or
- (d) Upon changes to the supplier's organizational structure or environment.

Supplemental Guidance: An assessment and review of supplier risk includes security and supply chain risk management processes, foreign ownership, control or influence (FOCI), and the ability of the supplier to effectively assess subordinate second-tier and third-tier suppliers and contractors.

Agencies can use open-source information to monitor for indications of stolen information, poor development and quality control practices, information spillage, or counterfeits.

Agencies should review the US Department of Commerce Bureau of Industry and Security [Lists of Parties of Concern](#), the International Trade Association [Consolidated Screening List](#), and the National Defense Authorization Act (NDAA) [Section 889](#) prior to contracting with a supplier. In general, the NJ Office of Homeland Security and Preparedness prohibits agencies from purchasing systems, system components, and services from companies on these lists due to threats they pose to the State and/or Nation. Agencies should contact the NJCCIC for further guidance.

## **SU-07: NOTIFICATION AGREEMENTS**

Agencies shall establish agreements and procedures with entities involved in the system, system component, or system service supply chain requiring notification of supply chain compromises; results of assessments or audits; and remediation plans, as applicable.

Supplemental Guidance: The establishment of agreements and procedures facilitates communications among supply chain entities. Early notification of compromises and potential compromises in the supply chain that can potentially adversely affect or have adversely affected agency systems or system components is essential for organizations to effectively respond to such incidents. The results of assessments or audits may include open-source information that contributed to a decision or result and could be used to help the supply chain entity resolve a concern or improve its processes.

## **SU-08: INSPECTION OF SYSTEMS OR COMPONENTS**

Upon receipt of systems and/or systems components, the receiving agency must inspect the packaging, bill of lading, packing slip, systems and/or system components for any signs of tampering to the system or systems components.

Supplemental Guidance: Agencies should develop processes to inspect systems and systems components any time the system or component is removed from agency-controlled areas (e.g. system and components sent out for repair and returned to the agency) and/or when individuals return from travel to high-risk areas. Indications of a need for inspection include changes in packaging, specifications, factory location, or entity in which the part is purchased.

## **SU-09: COMPONENT AUTHENTICITY**

Agencies shall:

- (a) Not knowingly procure counterfeit systems or system components;
- (b) Employ a risk-based approach to reduce the frequency and impact of counterfeit systems or system components within agency acquisitions and agency life-cycle sustainment processes by:

1. Applying prevention and early detection procedures to minimize the presence of counterfeit components within the agency supply chain as the primary strategy in eliminating counterfeit materiel within the agency;
  2. Strengthening the oversight and surveillance procedures for critical and sensitive systems and system components; and
  3. Maintaining configuration control over system components awaiting service or repair and serviced or repaired components awaiting return to service.
- (c) Document all occurrences of suspect and confirmed counterfeit systems and system components;
- (d) Investigate, analyze, and assess all cases of suspected counterfeit systems and systems components;
- (e) Notify agency management, the NJCCIC, NJOIT, the Division of Purchase and Property, and the source of the counterfeit component;
- (f) Seek restitution when cases are confirmed; and
- (g) Provide agency staff with anti-counterfeit education and training to include responsibilities and processes for inspection and reporting of suspected counterfeit systems and system components.

Supplemental Guidance: Sources of counterfeit components include manufacturers, developers, vendors, and contractors. Anti-counterfeiting policies and procedures support tamper resistance and provide a level of protection against the introduction of malicious code.

## **SU-10: COMPONENT DISPOSAL**

In accordance with all applicable State and Federal laws, executive orders, circulars, directives, and policies regarding the disposal of systems and system components, agencies shall first [sanitize](#) all media containing sensitive information, software, documentation, etc., from systems and system components prior to disposal.

Supplemental Guidance: Data, documentation, tools, or system components can be disposed of at any time during the system development life cycle (not only in the disposal or retirement phase of the life cycle). Opportunities for compromise during disposal affect physical and logical data, including system documentation in paper-based or digital files; shipping and delivery documentation; memory sticks with software code; or complete routers, servers, and multi-function devices that include permanent media, and may contain sensitive or proprietary information.

## **REFERENCES**

The requirements established in the Supply Chain Risk Management policies and standards have been derived from the following references:

NIST SP 800-53r5: Supply Chain Risk Management (SU); Systems and Services Acquisition (SA); and

NIST CSF: Identify – Business Environment (ID-BE); Protect – Awareness and Training (PR-AT); Identify – Governance (ID-GV); Identify – Supply Chain (ID-SC).

---

## ASSESSMENT, AUTHORIZATION, AND MONITORING (CA)

---

### CA-01: PURPOSE

The purpose of the Assessment, Authorization, and Monitoring policies and standards is to ensure that the security controls for State information systems are assessed and risks are managed to acceptable levels throughout their lifecycles.

### KEY TERMS

**External Connections** - System or IP addressable end points that are not under the direct control of the Executive Branch of New Jersey State Government, systems that have IP addressing not in the Executive Branch's addressing scheme (routable and non-routable), or systems that have an authorizing official who is not an Executive Branch employee.

**General Support System** - A general support system is an interconnected set of information resources under the same direct management control that shares common functionality. A general support system normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. A general support system, for example, can be a:

- Local area network (including workstations, printers, and other assets that support an agency office or facility);
- Backbone network (e.g. agency-wide and/or statewide (GSN));
- Agency data processing center including its operating system and utilities (e.g. server room); and/or
- Shared information processing service facility (e.g. data center).

**Major Applications and Systems** – A major application or system is described as any system or application that includes one or more of the following characteristics:

- Includes users in more than one agency;
- Costs more than \$100,000 to develop and implement (cost includes hardware, software, and contract personnel);
- Any public-facing web application; and/or
- Any application that stores or processes sensitive information or is deemed critical to the operations of the agency.

**System Security and Privacy Plan** - A formal document that provides an overview of the security and privacy requirements for an information system and describes the controls in place, or planned, for meeting those requirements.

## CA-02: POLICY

All major systems and applications and general support systems are required to undergo security assessments to ensure adequate security and privacy controls are implemented and risks are managed to acceptable levels throughout their lifecycles.

## CA-03: CONTROL ASSESSMENTS

As part of the NJOIT SAR process, the NJCCIC in coordination with NJOIT and Agency Information Security, Privacy, and Technology personnel shall:

- (a) Conduct assessments for all new major applications, general support systems, and external connections, as well as any major applications, general support systems, and external connections in development or undergoing substantive changes to ensure adequate security and privacy controls are implemented and risks are managed to acceptable levels prior to placement into an operational status;
- (b) As feasible and necessary, engage independent security assessors;
- (c) Document the results of the assessment;
- (d) Provide the results of the security and privacy controls assessment, in writing, to the Agency's Information Security Official and the State Chief Information Security Officer; and
- (e) Periodically reassess the system to determine any deviations its state of compliance and that which is required.

For an information system that is not considered to be a major application, general support system, or has external connections, agency information security, privacy, and technology personnel shall be responsible for assessing and maintaining appropriate security and privacy control throughout the life cycle of the system.

Supplemental Guidance: Risk management processes including identifying, assessing, and addressing security and privacy risks at the inception of the project to build a system until the decommissioning of a system, which enables agencies to maintain security and privacy of a system throughout its lifecycle. To aid in satisfying the ongoing assessment requirements, agencies can use assessment results from the following sources: continuous monitoring, audits and authorizations, and other system development life cycle activities.

## CA-04: INFORMATION EXCHANGE

Agencies, in coordination with NJOIT, the NJCCIC, and in accordance with [State of New Jersey IT Circular, 09-11-NJOIT, Extranet Policy](#) shall:

- (a) Approve and manage the exchange of information between the system and other systems using appropriate interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements; or other appropriate agreement vehicle;

- (b) Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and
- (c) Review and update the agreements at least annually or any time changes are made with respect to the information exchange parameters.

Supplemental Guidance: This control applies to dedicated connections between information systems and does not apply to transitory, user-controlled connections such as website browsing. System information exchange requirements apply to information exchanges between two or more systems. System information exchanges include connections via leased lines or virtual private networks, connections to internet service providers, database sharing or exchanges of database transaction information, connections and exchanges with cloud services, exchanges via web-based services, or exchanges of files via file transfer protocols, network protocols (e.g., IPv4, IPv6), email, or other organization-to-organization communications.

Agency management determines the risk associated with system information exchange and the controls needed for appropriate risk mitigation. The types of agreements selected are based on factors such as the impact level of the information being exchanged, the relationship between the organizations exchanging information (e.g., government to government, government to business, business to business, government or business to service provider, government or business to individual), or the level of access to the system by users of the other system. Agencies may incorporate agreement information into formal contracts, especially for information exchanges established between state agencies and non-state organizations (including local, municipal and Federal government organizations, service providers, contractors, system developers, and system integrators).

## **CA-05: PLAN OF ACTION AND MILESTONES**

Agency asset owners and asset custodians shall:

- (a) Develop a plan of action and milestones for the system to document the planned remediation actions to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and
- (b) Update existing plan of action and milestones based on the findings from subsequent control assessments, independent audits or reviews, and continuous monitoring activities.

Supplemental Guidance: Plans of action and milestones, also referred to as corrective action plans, should be used to track planned remedial actions.

## **CA-06: AUTHORIZATION**

Agency chief information security and privacy officers in coordination with the agency chief information officer are responsible for authorizing the systems to operate prior to introduction into the production environment; and

- (a) Updating the authorization on an ongoing basis, consistent with applicable control requirements and statutory and regulatory obligations.
- (b) For systems that are considered critical and/or sensitive, the State Chief Information Security Officer and the State Chief Information Technology Officer, or their delegates may act as authorizing officials.

## **CA-07: CONTINUOUS MONITORING**

In order to establish and maintain situational awareness and the ability to address new threats to the security and privacy of a system, agencies are responsible for implementing continuous monitoring processes. Information system owners, asset custodians, and agency information security personnel in coordination with the NJCCIC shall:

- (a) In accordance with the audit and accountability requirements, implement processes to monitor the system security logs and events;
- (b) Forward the system's security event logs to and engage the NJCCIC aiding in the identification and management of threats and assessment of risks to the system;
- (c) Conduct ongoing security assessments of information systems and information;
- (d) Conduct ongoing security assessments and vulnerability scans;
- (e) Initiate response actions and apply security patches to address results of the security assessments, vulnerability scans, and system monitoring; and
- (f) Periodically report the security and privacy status of the system to agency management.

Supplemental Guidance: Continuous monitoring at the system level facilitates ongoing awareness of the system security and privacy posture to support agency risk management decisions. The terms "continuous" and "ongoing" imply that agencies assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions. Different types of controls may require different monitoring frequencies.

## **CA-08: PENETRATION TESTING AND RED TEAM EXERCISES**

Prior to the scheduling, contracting, or conducting penetration tests, red team exercises, vulnerability scans, compromise assessments, and other security tests against State information systems, agency management shall coordinate and must receive explicit approval for all security testing from the State Chief Information Security Officer.

Supplemental Guidance: Penetration testing is a specialized type of assessment conducted on systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Penetration testing goes beyond automated vulnerability scanning and is conducted by agents and teams with demonstrable skills and experience that include technical expertise in network, operating system, and/or application-level security. Red team exercises extend the objectives of penetration testing by examining the security and privacy posture of agencies and the capability to implement effective cyber defenses. Red team exercises simulate attempts by adversaries to compromise mission and business functions. Penetration tests, red team

exercises, compromise assessments, and vulnerability scans can have adverse collateral impacts to the performance and security of other State information systems and networks.

## **CA-09: INTERNAL SYSTEM CONNECTIONS**

Agency information security, privacy, and technology officials shall assess risks and authorize as appropriate internal and external connections including, for example, system connections with mobile devices, notebook and desktop computers, tablets, printers, copiers, facsimile machines, scanners, sensors, and servers.

Supplemental Guidance: Rather than authorizing each internal system connection individually, agencies should authorize connections for a class of system components with common characteristics and/or configurations, including printers, scanners, and copiers with a specified processing, transmission, and storage capability or smart phones and tablets with a specific baseline configuration.

## **REFERENCES**

The requirements established in the Assessment, Authorization, and Monitoring Policy and standards have been derived from the following:

- NIST SP 800-53r5 Assessment, Authorization, and Monitoring (CA); and
- NIST CSF Identify/Risk Assessment (ID.RA), Identify/Risk Management (ID.RM), Detect/Security Continuous Monitoring (DE.CM).

---

## AUDIT AND ACCOUNTABILITY (AU)

---

### AU-01: PURPOSE

The purpose of the Audit and Accountability policies and standards is to establish and maintain situational awareness within individual agencies, and across the Executive Branch as a whole, through timely collection and review of security-related event logs.

### KEY TERMS

**Audit Log** - A chronological record of system activities. Includes records of system accesses and operations performed in a given period.

**Component** - A general term that is used to mean one part of something more complex. Scope Note: For example, a computer system may be a component of an IT service, or an application may be a component of a release unit. Components are co-operating packages of executable software that make their services available through defined interfaces. Components used in developing systems may be commercial off-the-shelf software (COTS) or may be purposely built. However, the goal of component-based development is to ultimately use as many pre-developed, pretested components as possible.

**Event** - Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring.

**Incident** - An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

### AU-02: AUDIT AND ACCOUNTABILITY POLICY

Agency asset owners, asset custodians, and information security and privacy officers shall:

- (a) Ensure the information assets under their purview are assessed for security and privacy risks and configured such that event logging is enabled to ensure an adequate level of situational awareness regarding potential threats to the confidentiality, integrity, availability, and privacy of agency information and information systems are identified and managed; and
- (b) Review and retain event logs in compliance with all applicable State and Federal laws, regulations, executive orders, circulars, directives, internal agency and State of New Jersey policies, and contractual requirements.

## **AU-03: AUDIT EVENTS**

Asset Custodians and information security personnel shall:

- (a) Implement processes to capture, protect, and review security event logs from all system components (network devices, workstations, servers, applications, databases, etc.) to identify and manage suspicious activity within their respective agencies; and
- (b) Forward their security event logs to the NJCCIC in order to aid in identifying and managing threats to individual agencies, and to correlate events across all agencies that comprise the Executive Branch.

Supplemental Guidance: An event is an observable occurrence in a system. The types of events that require logging are those events that are significant and relevant to the security of systems and the privacy of individuals. Event logging also supports specific monitoring and auditing needs. Event types include password changes, failed logons or failed accesses related to systems, security or privacy attribute changes, administrative privilege usage, PIV credential usage, data action changes, query parameters, or external credential usage. In determining the set of event types that require logging, agencies should consider the monitoring and auditing appropriate for each of the controls to be implemented. For completeness, event logging includes all protocols that are operational and supported by the system. Conducting reviews of security-related events within an individual agency and forwarding the logs of the events to the NJCCIC provides both a compartmentalized view and a holistic view of events across the Executive Branch of New Jersey State Government. These include events such as successful and failed login activity; data requests, data transfers; changes to configuration files; the addition, deletion, or modification of User-IDs, etc.

Without comprehensive visibility into infrastructure, operating system, database, application and other logs, the State will have gaps in its situational awareness that could lead to system compromise and/or data exfiltration. Event logging and monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security that support risk management decisions.

## **AU-04: CONTENT OF AUDIT RECORDS**

Agency Asset Custodians shall: ensure audit records from systems and system components establish the following:

- (a) What type of event occurred;
- (b) When the event occurred;
- (c) Where the event occurred;
- (d) Source of the event;
- (e) Outcome of the event; and
- (f) Identity of any individuals, subjects, or objects/entities associated with the event.

Examples of events that are to be collected and forwarded to the NJCCIC include, but are not limited to the following:

(a) Operating System Events:

1. Start up and shut down of the system;
2. Start up and down of a service;
3. Network connection changes or failures; and
4. Changes to, or attempts to change, system security settings and controls.

(b) Operating System Audit Records:

1. Logon attempts (successful or unsuccessful);
2. The function(s) performed after logged on (e.g., reading or updating critical files, software installation);
3. Account changes (e.g., account creation and deletion, account privilege assignment); and
4. Successful/failed use of privileged accounts.

(c) Application Account Information:

1. Successful and failed application authentication attempts;
2. Application account changes (e.g., account creation and deletion, account privilege assignment); and
3. Use of application privileges.

(d) Application Operations:

1. Application startup and shutdown;
2. Application failures;
3. Application configuration changes; and
4. Application transactions, for example:
  - a) Email servers recording the sender, recipients, subject name, and attachment names for each email;
  - b) Web servers recording each URL requested and the type of response provided by the server; and
  - c) Applications recording what sensitive information accessed by each user.

(e) Logs of all systems and system components that perform security functions. This includes, but is not limited to:

1. Endpoint Detection and Response Software;
2. Network and Web Application Firewalls;
3. Intrusion Detection and Prevention Systems (IDS/IPS);
4. DDOS Protection Systems;

5. Web and Email filtering Systems;
6. Authentication servers (e.g. Active Directory, LDAP servers, Cloud apps);
7. VPN and Remote Access systems and services; and
8. DNS servers.

Supplemental Guidance: Agencies are encouraged to review [NIST Special Publication 800-92, Guide To Security Log Management](#) for more information on audit log content.

## **AU-05: PERSONALLY IDENTIFIABLE INFORMATION IN AUDIT LOGS**

Agencies are to limit personally identifiable information contained in audit logs to that documented in the System Security and Privacy Plan for the auditing and logging system.

## **AU-06: AUDIT LOG STORAGE CAPACITY**

The State Chief Information Security Officer shall be responsible for ensuring that the enterprise log aggregation system stores all audit log content for a minimum of one (1) year.

Supplemental Guidance: The NJCCIC has procured and implemented a log aggregation system that can store logs for one year. Agencies that have statutory, regulatory, and/or contractual obligations to store audit logs for more than one year should contact NJCCIC and NJOIT management to coordinate the archiving of historical logs. For more information on retention requirements, Agencies should refer to State of New Jersey, Chapter 410, Laws of 1953, [Destruction of Public Records Act](#), and the [State General Records Retention Schedule](#).

## **AU-07: RESPONSE TO AUDIT LOGGING PROCESS FAILURES**

In the event of an audit log processing failure, such as software/hardware errors with the audit capturing mechanisms, agencies shall:

- (a) Ensure systems are configured to send alerts to the appropriate agency asset custodians for the system(s) that experienced the failures.
- (b) Ensure asset custodians for those systems take corrective actions to resolve the issue(s) causing the log processing failure.

## **AU-08: AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING**

Agency asset custodians, agency information security and NJCCIC personnel shall:

- (a) Continuously review and analyze system audit records for indications of suspicious activity, generated security alerts, and other inappropriate or anomalous activity; and
- (b) Report suspected incident findings in accordance with incident reporting processes.

Supplemental Guidance: The NJCCIC maintains a Security Operations Center (SOC) where it monitors security telemetry for all State information systems. It also maintains a centralized log aggregation system that allows it to correlate and/or reconstruct events that occur over time and to satisfy State and Federal statutory, regulatory, and contractual requirements regarding log

retention. In addition, it engages a third-party information security and analysis center to provide 24/7 monitoring and alerting of State systems and networks.

## **AU-09: AUDIT REDUCTION AND REPORT GENERATION**

The State Chief Information Security Officer is responsible for implementing a log aggregation system. Asset custodians and asset owners shall ensure information assets are configured to:

- (a) Support on-demand and batch/scheduled report generation, record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and
- (b) Do not alter the original content or time ordering of audit records.

Supplemental Guidance: Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit reduction and report generation capabilities do not always emanate from the same information system or from the same organizational entities conducting auditing activities. Audit reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. Time ordering of audit records can be a significant issue if the granularity of the timestamp in the record is insufficient.

## **AU-10: TIME STAMPS**

Asset custodians shall configure all systems and applications to use the Network Time Protocol (NTP) and the NJOIT's approved time sources to ensure clocks are synchronized and log file timestamps are accurate.

Supplemental Guidance: Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. NTP is an Internet standard protocol which enables client computers to maintain system time synchronization. To ensure time is synchronized across all systems on the GSN, agencies should use NJOIT's time servers.

Granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks (e.g., clocks synchronizing within hundreds of milliseconds or tens of milliseconds). Time service can be critical to security capabilities, such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities.

## **AU-11: PROTECTION OF AUDIT RECORDS**

Audit records are to be protected and retained in accordance with their sensitivity and all applicable State and Federal laws, regulations, executive orders, circulars, directives, contracts, and State and agency-specific policies.

- (a) NJCCIC asset custodians are required to implement safeguards to protect the audit records in the enterprise log aggregation system from unauthorized access, modification, and deletion;

- (b) Audit records in the enterprise log aggregation system shall be restricted to personnel routinely responsible for performing security audit functions; and
- (c) Audit logs are to be retained for a minimum of one (1) year. in accordance with all State and Federal laws, regulations, contracts, and internal agency policies governing their retention.

Supplemental Guidance: Agencies that have statutory, regulatory, and/or contractual obligations to store audit logs for more than one year should contact NJCCIC and NJOIT management to coordinate the archiving of historical logs. For more information on retention requirements, Agencies should refer to State of New Jersey, Chapter 410, Laws of 1953, [Destruction of Public Records Act](#), and the [State General Records Retention Schedule](#).

## REFERENCES

The requirements established in the Audit and Accountability policies and standards have been derived from following:

- NIST SP 800-53 Audit and Accountability (AU), System and Information Integrity (SI);
- NIST CSF Protect/Protective Technologies (PR.PT), Detect/Continuous Monitoring (DE.CM), Detect/Detection Processes (DE.DP); and
- [NIST Special Publication 800-92, Guide To Security Log Management](#).

---

## MAINTENANCE (MA)

---

### MA-01: PURPOSE

The purpose of the Maintenance policies and standards is to ensure that information assets are properly maintained, thereby minimizing the risks from emerging information security threats and/or the potential loss of confidentiality, integrity, or availability due to system failures.

### KEY TERMS

**Asset Custodian** - A person or group responsible for the day-to-day management, operation, and security of an asset. An asset custodian typically has a role of system, database, or network administrator. Asset custodian is synonymous with data or information custodian.

**Asset Owner** - A person or organizational unit (internal or external to the organization) with primary responsibility for the viability, productivity, security, and resilience of an organizational asset. The term Asset Owner is synonymous with Information System Owner and System Owner.

### MA-02: MAINTENANCE POLICY

In order to minimize risk from evolving threats and maintain system availability, the periodic and ongoing maintenance and upgrades of agency information assets shall be performed at predetermined, authorized times or on an approved, as-needed basis.

Asset custodians in collaboration with asset owners shall:

- (a) Develop and implement system maintenance procedures and schedules;
- (b) Prioritize maintenance of mission critical and sensitive systems and components;
- (c) Proactively obtain maintenance support and spare parts for critical systems;
- (d) Ensure maintenance is performed in accordance with applicable laws, regulations, State and agency policies, and contractual requirements;
- (e) Conduct maintenance in a timely manner to minimize downtime and business disruption; and
- (f) Document performed maintenance and regularly review and adjust maintenance schedules in order to mitigate risks to agency information systems and information.

Supplemental Guidance: Agencies should determine if maintenance operations represent configuration changes and follow configuration change processes, if applicable.

### MA-03: CONTROLLED MAINTENANCE

Asset custodians in collaboration with asset owners and agency management shall:

- (a) Schedule, document, and review records of maintenance, repair, and replacement of system components in accordance with manufacturer or vendor specifications and/or agency requirements;

- (b) Approve and monitor all maintenance activities, whether performed on-site or remotely and whether the system or system components are serviced on-site or moved to another location;
- (c) Require that agency management explicitly approves the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;
- (d) Sanitize equipment to remove the sensitive information from associated media prior to removal from agency facilities for off-site maintenance, repair, or replacement;
- (e) Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and
- (f) Include the following information in organizational maintenance records:
  - 1. Date and time of maintenance;
  - 2. Description of maintenance performed;
  - 3. Names of individuals or groups performing maintenance;
  - 4. Name of escort; and
  - 5. System components equipment that is removed or replaced.

Supplemental Guidance: Controlling system maintenance addresses the information security aspects of the system maintenance program and applies to all types of maintenance to system components conducted by local or nonlocal entities. Maintenance includes peripherals, such as scanners, copiers, and printers.

## **MA-04: MAINTENANCE TOOLS**

Asset custodians in collaboration with asset owners, information security personnel, and agency management shall:

- (a) Approve, control, and monitor the use of system maintenance tools;
- (b) Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications;
- (c) Check media containing diagnostic and test programs for malicious code before the media are used in an agency system;
- (d) Prevent the removal of maintenance equipment containing agency information by:
  - 1. Verifying that there is no sensitive agency information contained on the equipment;
  - 2. Sanitizing or destroying the equipment;
  - 3. Retaining the equipment within the facility; or
  - 4. Obtaining an exemption from agency management explicitly authorizing removal of the equipment from the facility.

- (e) Periodically review previously approved system maintenance tools.

Supplemental Guidance: Approving, controlling, monitoring, and reviewing maintenance tools address security-related issues associated with maintenance tools that are not within system authorization boundaries and are used specifically for diagnostic and repair actions on agency systems. Agencies have flexibility in determining roles for the approval of maintenance tools and how that approval is documented. A periodic review of maintenance tools facilitates the withdrawal of approval for outdated, unsupported, irrelevant, or no-longer-used tools. Maintenance tools can include hardware, software, and firmware items and may be pre-installed, brought in with maintenance personnel on media, cloud-based, or downloaded from a website. Such tools can be vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into systems. Maintenance tools can include hardware and software diagnostic test equipment and packet sniffers.

Maintenance tools can be directly brought into a facility by maintenance personnel or downloaded from a vendor's website. If, upon inspection of the maintenance tools, the agency determines that the tools have been modified in an improper manner or the tools contain malicious code, the incident is to be handled consistent with applicable incident handling policies and procedures.

## **MA-05: NONLOCAL MAINTENANCE**

Agencies are required to:

- (a) Approve and monitor nonlocal maintenance and diagnostic activities;
- (b) Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;
- (c) Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;
- (d) Maintain records for nonlocal maintenance and diagnostic activities; and
- (e) Terminate session and network connections when nonlocal maintenance is completed.

Supplemental Guidance: Nonlocal maintenance and diagnostic activities are conducted by individuals who communicate through either an external or internal network. Local maintenance and diagnostic activities are carried out by individuals who are physically present at the system location and not communicating across a network connection. Strong authentication (Multi-Factor Authentication) should be required for all nonlocal maintenance and diagnostic sessions.

## **MA-06: MAINTENANCE PERSONNEL**

Agencies are required to:

- (a) Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;

- (b) Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and
- (c) Designate agency personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

## **REFERENCES**

The requirements established in the Maintenance policies and standards have been derived from the following:

- NIST SP 800-53r5 Maintenance (MA); and
- NIST CSF Protect/Maintenance (PR-MA);

---

## PLANNING (PL)

---

### PL-01: PURPOSE

The purpose of the Planning policies and standards is to ensure that due care security and privacy planning considerations are addressed to effectively and efficiently manage risks to State information systems and information.

### KEY TERMS

None. See Glossary for a complete listing of terms

### PL-02: POLICY

As part of the NJOIT System Architecture Review process, agencies shall submit security and privacy plans for all new systems and systems undergoing major changes. The submitted plans shall establish the roles, responsibilities, controls, policies, and procedures that address the security and privacy requirements of the system and are consistent with applicable state and federal laws, executive orders, directives, regulations, policies, standards, and contractual obligations. At a minimum, the submitted security and privacy plans shall include a System Security and Privacy Plan (SSPP) that is to be developed by the NJCCIC.

### PL-03: SYSTEM SECURITY AND PRIVACY PLAN

System Security and Privacy Plans (SSPPs) are a means to document security and privacy requirements and associated security and privacy controls implemented within a given system. The State Chief Information Security Officer in coordination with the State Chief Technology Officer shall develop enterprise-wide SSPP requirements. The SSPP shall:

- (a) Be consistent with the State's enterprise architecture;
- (b) Explicitly define the constituent system components;
- (c) Describe the operational context of the system in terms of mission and business processes;
- (d) Identify the individuals that fulfill system roles and responsibilities;
- (e) Identify the information types processed, stored, and transmitted by the system;
- (f) Provide the security categorization of the system, including supporting rationale;
- (g) Describe any specific threats to the system that are of concern to the agency/State;
- (h) Provide the results of a privacy risk assessment for systems processing personally identifiable information;
- (i) Describe the operational environment for the system and any dependencies on or connections to other systems or system components;
- (j) Provide an overview of the security and privacy requirements for the system;

- (k) Identify any relevant control baselines or overlays, if applicable;
- (l) Describe the controls in place, or planned, for meeting the security and privacy requirements, including a rationale for any tailoring decisions;
- (m) Include risk determinations for security and privacy architecture and design decisions;  
and
- (n) Include security- and privacy-related activities affecting the system that require planning and coordination with the NJOIT and the NJCCIC.

## **PL-04: COMPLETION AND SUBMISSION OF THE SYSTEM SECURITY AND PRIVACY PLAN**

Agencies shall:

- (a) Submit an SSPP for new information systems, systems under development, systems undergoing changes or upgrades, or other activities that pose a privacy risk;
- (b) Ensure an SSPP is conducted prior to any new collection of PII, or upon significant changes to any system in which security and privacy risks exist;
- (c) Submit the SSPP as part of the State's [System Architecture Review](#) process;
- (d) Use the SSPP to identify and implement appropriate controls; and
- (e) Protect the completed SSPP from unauthorized disclosure.

Supplemental Guidance: The System Architecture Review (SAR) is a process that brings sponsors, administrators and technologists together to help ensure that technology solutions for the State of New Jersey are conceived, designed, developed, and deployed in an effective, secure, and efficient manner, to maximize the benefits and functionality of the technology and align information technology investments with business needs at the Enterprise level, while minimizing its cost and risk. Participation in the SAR process informs:

- Cybersecurity and privacy requirements.
- Cross-Agency interoperability of systems.
- Data sharing and reuse.
- Opportunities to leverage economies of scale and/or existing solutions.
- Impact on existing technology infrastructure and operations.
- Prioritization of resource staff levels.
- Disaster recovery and business continuity requirements.

## **PL-05: RULES OF BEHAVIOR**

The use of State information assets is permitted for authorized State government business purposes to support the goals and objectives of the Executive Branch of New Jersey State Government departments and agencies. Accordingly, State information assets are to be used in

a manner that is consistent with applicable laws and regulations, in accordance with all New Jersey State Government policies, and as part of the individual's assigned duties and responsibilities.

## **PL-05.1: AGENCY RESPONSIBILITIES**

Agencies shall:

- (a) Establish and provide to individuals requiring access to a system, the rules that describe their responsibilities and expected behavior for the information and system usage, security, privacy, use of social media, posting organizational information on public websites, and use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications;
- (b) Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;
- (c) Review and update the rules of behavior at agency-defined frequencies; and
- (d) Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge the current version when the rules are revised or updated.

## **PL-05.2: USER REQUIREMENTS**

The rules of behavior and requirements contained in this Manual apply to all users of State information assets, regardless of the agency, role, or location. All uses of State information assets must comply with State of New Jersey policies, standards, procedures, and guidelines, as well as all applicable Federal and State laws. Certain users, subject to approval from agency management, may be exempted from certain requirements during the course of their legitimate job responsibilities. The following list of user requirements is by no means exhaustive, but attempts to provide a framework for activities which fall into the categories of generally acceptable and unacceptable use.

- (a) Users are responsible for protecting State information and resources from unauthorized use or disclosure;
- (b) Individuals who are provided with portable information assets including, but not limited to: laptop computers, tablets, smart phones, removable media, etc., shall be responsible for the physical security and condition of these information assets;
- (c) Users shall immediately report lost or stolen State information assets, suspected policy violations, suspected information security incidents, and suspicious activity, in accordance with their agency's reporting procedures;
- (d) Users are prohibited from performing any act that is illegal or otherwise in violation of any applicable Federal or State laws, or State policies;

- (e) Users are prohibited from accessing State information and/or systems without express authorization;
- (f) Users are prohibited from sharing account passwords, Personal Identification Numbers (PINs), security questions/answers, security tokens (e.g., smartcard, key fob), or similar information or devices used for authentication and authorization to State information assets;
- (g) Users are prohibited from engaging in the subversion of existing security controls unless expressly authorized by the State Chief Information Security Officer or his/her designee (e.g. network, computer or device hacking and scanning, password cracking, penetration testing, and conducting red team exercises, etc.);
- (h) Users are prohibited from purposely introducing malicious programs into the network or server (e.g., malware, viruses, worms, trojan horses, etc.);
- (i) Users are prohibited from accessing, transmitting, storing, or creating any discriminatory, defamatory, offensive, disruptive or otherwise inappropriate content including, but not limited to: websites that contain sexually suggestive images or content, racial slurs, gender specific comments, or any other comments that inappropriately or unprofessionally address someone's age, race, gender, color, national origin, religion, sexual orientation, disability, or veteran status;
- (j) Users are prohibited from creating, sending, and forwarding unsolicited email messages, including the sending of junk mail, chain letters, Ponzi or pyramid schemes, or other advertising material to individuals who did not specifically request such material (email spam);
- (k) Users are prohibited from sending email under another individual's name or email address, except when authorized to do so by the owner of the email account for a work-related purpose;
- (l) Users are prohibited from installing, downloading, or running software that has not been approved following appropriate review in accordance with State procurement policies;
- (m) Users are prohibited from adding or installing personal information technology resources (e.g. wireless access points, software, mobile devices, etc.) to existing State information systems without the appropriate management authorization;
- (n) Users are prohibited from establishing new Internet web and/or social media pages, accounts, or content dealing with State business, or make modifications to existing pages, accounts, or content dealing with State business without express authorization by agency management;
- (o) Users are prohibited from transmitting, storing, processing, or sharing sensitive State information using personal or other unauthorized Internet services including, but not limited to: personal email accounts, social media accounts, chat services, file storage, file synchronization, file sharing, and other unauthorized services;
- (p) Users are prohibited from sharing sensitive information without authorization;

- (q) Users are prohibited from purposely acquiring, using, reproducing, transmitting, or distributing any information, software or other electronic materials (e.g. movies, music) in violation of applicable copyright, trademark, intellectual property laws and contractual agreements;
- (r) Users are prohibited from using State information assets to conduct or promote user's outside employment or business interests;
- (s) Users are prohibited from using State information assets to conduct political activity such as lobbying elected officials and participating in partisan political activities without authorized approval; and
- (t) Users are prohibited from using State information assets to circulate unauthorized solicitations or advertisements for non-State purposes including religious, political, or not-for-profit entities.

## **PL-06: SECURITY AND PRIVACY ARCHITECTURE**

The State Chief Information Security Officer in coordination with the State Chief Technology Officer and other key stakeholders shall develop, document, and establish a security and privacy architecture that is incorporated into the overall enterprise information technology architecture. The security and privacy architecture shall be comprised of all the elements of the overall security and privacy program including the people, policies, processes, standards, guidelines and technologies that enable the secure transaction of business, delivery of services, communications and protection of information. The security and privacy architecture shall provide a risk-based, cost-effective framework, and foundation to enable secure communications, protect the State's business processes, information systems and information, and ensure that new methods for delivering service are secure.

The security and privacy architecture is guided by the following principles:

- (a) Information security and privacy supports the State's mission, strategies, goals and objectives;
- (b) Information security and privacy controls should be appropriate and commensurate to the value of and degree of reliance on the State's information technology resources and sufficient to contain risk at an acceptable level;
- (c) Information security and privacy requires a comprehensive and integrated approach;
- (d) Information security and privacy responsibilities and accountability should be made explicit;
- (e) Information security and privacy should be periodically reassessed and continually improved; and
- (f) Information security and privacy shall accommodate varying security needs.

## **PL-07: CENTRAL MANAGEMENT**

The State of New Jersey maintains an information security and privacy program that is centrally managed and coordinated via the New Jersey Cybersecurity and Communications Integration Cell in the New Jersey Office of Homeland Security and Preparedness and executed locally in each of the departments, agencies, commissions, boards, bodies, and other instruments of the Executive Branch of New Jersey State Government.

In accordance with the Organizational Security Policy, the State Chief Information Security Officer, who reports to the Director of the New Jersey Office of Homeland Security and Preparedness, shall establish and manage an information security program to ensure the confidentiality, integrity, and availability of the State of New Jersey Executive Branch's information resources, systems, and services while promoting and protecting privacy and safety. The State CISO has overall responsibility for the development, implementation, and performance of the information security program by:

- (a) Setting strategic information security planning across the Executive Branch of New Jersey State Government;
- (b) Publishing the Statewide Information Security Manual's policies and standards;
- (c) Developing, managing, and executing the Statewide Information Security Incident Response Plan;
- (d) Identifying security requirements to limit the risks associated with identified Executive Branch business objectives as defined by the Governor and the Heads of State agencies;
- (e) Developing, maintaining, and interpreting the Statewide Information Security Manual's Policies and Standards;
- (f) Providing information security subject matter expertise to State agencies;
- (g) Drafting and implementing an information security awareness and training program to be used by all State agencies;
- (h) Providing security metrics to track the performance of the information security program;
- (i) Developing an Information Security Governance, Risk, and Compliance program, including, but not limited to:
  - 1. Coordinating and conducting compliance and risk assessments of agencies and their information assets;
  - 2. Conducting and managing vulnerability assessments of agency networks, applications, databases, and systems;
  - 3. Conducting penetration tests of agency networks, applications, databases, and systems; and
  - 4. Conducting information security risk assessments of third parties with access to State of New Jersey information assets.

- (j) The policies, standards, procedures, and guidelines included in the Statewide Information Security Manual apply to all Departments, Agencies, Commissions, Boards, Bodies, or other instrumentalities of the Executive Branch of New Jersey State Government, hereinafter referred to as: agencies, the Executive Branch, the SoNJ, or the State. All Executive Branch full-time and part-time employees, temporary workers, volunteers, interns, contractors, and those employed by contracted entities - collectively referred to as users - are governed by and responsible for complying with the policies and standards regardless of agency, location, or role.

Supplemental Guidance: In addition, by [statute](#) and [executive order](#), information technology for the executive branch is centrally managed by the NJOIT under the direction of the State Chief Technology Officer.

## **PL-08: BASELINE SELECTION**

Agencies shall implement information security and privacy controls consistent with NIST SP 800-53r5 Moderate-Level controls as the baseline for all State information systems and information to ensure consistency throughout the Executive Branch and compliance with State and Federal statutes, executive orders, circulars, directives, regulatory, contractual, and other State policy requirements. Agencies may develop and implement a more restrictive set of information security and privacy policies and standards for use within their respective organization or for a specific information system, program, or requirement. Agency-developed information security policies and standards can exceed, but must not conflict with, the baseline established by this Manual.

## **PL-09: EXCEPTIONS TO BASELINE CONTROLS**

Agencies shall be responsible for documenting, approving and assuming any risk of loss of confidentiality, integrity or availability of an agency's information assets, due to the inability to comply with a policy or baseline control. The agency must fully describe the risk, and how the agency is ensuring that all necessary compensating controls have been implemented, and how the exception will be monitored.

All requests for compliance exceptions must be based on a valid restriction that prevents full compliance with the policy, standard, or procedure. All exception requests must be approved by the agency CIO or CISO and forwarded to the NJCCIC and the NJOIT for acceptance and cataloging.

### **PL-09.1: DOCUMENT EXCEPTION**

The requestor of an exception to a policy, standard, or procedure shall document, at a minimum, the following information in the Information Security Exception Request Form:

- (a) A specific description of the exception and the policy, standard, or procedure for which the exception is requested;
- (b) The reason why the policy, standard, or procedure cannot be implemented and the proposed alternative measures or compensating controls to be implemented;

- (c) The proposed exception duration with a specific date for remediation, which can be no longer than one year from the date of the exception request;
- (d) The criticality and/or sensitivity of data or hardware involved in the exception; and
- (e) The requestor will forward the request to their Agency CIO/CISO for approval and signature.

Supplemental Guidance: Agencies should maintain documentation describing the functional limitations and the mechanism employed to mitigate the risk. The exception shall be considered temporary and the NJCCIC shall track and review exceptions for as long as they exist, to determine if the exception is still required, if the Agency has the means to correct the exception, or if alternative mechanisms can be put in place to remediate the exception.

## **PL-09.2: REQUEST APPROVAL**

The agency CISO and his/her designated representatives will review the request from the agency requestor and, if they approve, will sign and forward to the State Chief Information Security Officer for review, via [riskreview@cyber.nj.gov](mailto:riskreview@cyber.nj.gov).

The State Chief Information Security Officer, or his/her designate, upon receiving the request for exception, shall:

- (a) Review and determine:
  - 1. The validity of the request as it relates to the overall Statewide Information Security Manual goals and objectives and any risk mitigation considerations or compliance mandates that impact the request;
  - 2. Whether the exception violates any dominant policy, statutory, regulatory, or known contractual compliance obligation (e.g., Federal, State);
  - 3. Whether the proposed alternative measures provide the appropriate compensating controls;
  - 4. Whether other alternative approaches for handling the requested exception may be available for consideration; and
  - 5. Whether the proposed plan and timeframe for corrective actions are reasonable given the risk.
- (b) Solicit input from key management and business units that may be affected by the exception.
- (c) Forward the exception to the NJOIT Information Security Officer, or his/her designate, for review with related systems managed by NJOIT, and for a coordinated decision. The NJOIT ISO shall:
  - 1. Determine the potential impact the exception request may have on any other NJOIT managed systems or the Garden State Network as a whole;

2. Indicate their approval if no expected extra-Agency security risks to NJOIT managed State assets exist;
  3. Indicate disapproval if there would be expected extra-Agency security risks to NJOIT managed State assets;
  4. Indicate conditional approval and specify any additional actions required by the requesting Agency in order to comply; and
  5. Return the request with their decision to the State CISO for final review and handling.
- (d) Accept the review from the NJOIT ISO, and coordinate with the agency CIO/CISO and the requestor to ensure that the appropriate alternative control methods agreed upon in granting the exception have been implemented and that the request is still valid. If approved, the exception is signed and returned to the agency CISO. If disapproved, the exception is returned to the requestor.
1. After final review, approve or disapprove the exception and notify the requestor, and also inform the State Chief Technology Officer and the NJOIT ISO. The NJCCIC shall maintain copies of, and track, all exceptions.
- (e) Review approved exceptions with the agency requestor on an ongoing basis (no less than annually), to determine if the exception is still required and valid.
- (f) Should the State Chief Information Security Officer disapprove the policy exception request, the requestor will have ninety (90) days to comply with the policy, standard, or procedure.
- (g) On an ongoing basis (no less than annually), the State Chief Information Security Officer or an authorized delegate is to review all outstanding exceptions with the agency CIO/CISO or requestor to determine if the exception is still required and valid.
- (h) Any policy exception request more than one (1) year old will require a new request be submitted for an updated review and determination.

## REFERENCES

The requirements established in the Planning policy and standards have been derived from the following:

- NIST SP 800-53r5 Planning; and
- NIST CSF Protect/Data Security (PR.DS).

---

## PHYSICAL AND ENVIRONMENTAL SECURITY (PE)

---

### PE-01: PURPOSE

The purpose of the Physical and Environmental Security policies and standards is to establish requirements to facilitate the implementation of the physical and environmental protections for State information systems and the facilities in which they are housed.

### KEY TERMS

**Authorization** - Access privileges granted to a user, program, or process, or the act of granting those privileges.

### PE-02: PHYSICAL AND ENVIRONMENTAL SECURITY POLICY

Agencies shall:

- (a) Establish documented physical controls and procedures that limit access to systems, equipment, and the respective operating environments to only authorized individuals; and
- (b) Provide appropriate environmental controls in facilities containing information systems and assets to ensure sufficient environmental conditions exist to avoid preventable hardware failures and service interruptions.

### PE-03: PHYSICAL ACCESS SECURITY ZONES

Agencies shall configure their premises into areas (zones) with differing levels of security as required to allow for access by authorized personnel. The fundamental principle behind this zoning is to have multiple layers of physical security protecting the most critical assets and services.

There are four (4) main categories of zones:

- (a) **Public Zone** - Areas of an agency facility accessible by the general public either by vehicles or on foot without prior control, such as grounds, parking lots, and other areas of the facility. Property limits should be clearly identified. Information deemed Moderate or High Risk, as defined in this Manual, must not be left unattended in Public Zones.
- (b) **Reception Zone** - An area at the entrance point of an agency facility where the initial contact with representatives of the agency occurs (e.g., receptionist, Physical Security personnel). Although certain basic business activities can be conducted in Reception Zones, their main purpose is to provide an adequate environment for identification and access control.

- (c) **Operations Zone** - A general access area where agency daily business activities or support services are regularly conducted. The basic security objective is to ensure that access and movement within this zone is limited to authorized personnel.

Access to operations zones requires appropriate credentials (visible ID badge, proximity card, combination, or keys) and is limited to:

1. Authorized employees (all employees of a particular location);
2. Authorized and adequately supervised contractors; and
3. Properly escorted visitors.

Access to an operations zone from a public zone should be properly labelled (e.g. "Restricted area. Employees only!")

- (d) **Restricted Access Zone** - An operational zone that requires specific authorization granted by the owner of each restricted zone. Restricted access zones could be areas such as data centers, server or computer rooms, cable cabinets, and communication equipment rooms. Not all operations zone personnel have access to restricted access zones. As a general rule, restricted access zones should not be directly accessible from public zones.

Restricted access zones include a combination of enhanced security measures to ensure that:

1. Access privileges are limited to specifically authorized employees, contractors, and escorted visitors based upon necessity;
2. Unauthorized access is detected, and prompt and appropriate intervention action is taken; and
3. The areas are monitored as a detective security control.

Controlling physical access to restricted access zones is required and access must be based on an individual's job function.

Access to restricted access zones must be revoked immediately upon termination, and all physical access mechanisms, keys, access badges, or tokens, must be returned or disabled.

Critical or sensitive information processing facilities shall be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls.

Supplemental Guidance: The security zone categories represent descriptions of their purpose.

## **PE-04: PHYSICAL ACCESS AUTHORIZATIONS**

Access to the non-public areas of agency facilities shall only be granted to authorized personnel.

- (a) Agencies shall develop, maintain, and periodically review lists of individuals that are provided access to Operations Zones and Restricted Access Zones.

- (b) Agency employees shall be provided authorized access to Operations Zones and Restricted Access Zones within agency facilities based on their roles and responsibilities;
- (c) Agencies are required to maintain records documenting the authorization and provisioning of physical access to agency facilities;
- (d) Agencies shall establish procedures to ensure employees and other authorized individuals understand the security procedures and safeguards related to the zones to which they have access; and
- (e) With the exception of areas that are designated as publicly accessible, agencies shall maintain a list of personnel with authorized access to a facility or a secured area within the facility where agency information assets reside.

### **PE-05: VISITOR CONTROL**

Physical access to the Operations Zones and Restricted Access Zones of agency facilities by visitors shall be restricted and controlled in order to prevent unauthorized access to agency information assets. Other than areas designated as publicly accessible, all visitors shall be approved and authenticated before access to agency Operations Zones or Restricted Access Zones.

Individuals escorting visitors are responsible for ensuring that the visitors:

- (a) Wear their visitor security badge at all times; and
- (b) Are escorted until they are signed out.

### **PE-06: LOST OR STOLEN ID BADGES**

Agencies shall establish procedures for badge holders to report any loss or theft of their ID badge. Lost or stolen badges are to be immediately deactivated to prevent unauthorized access to agency facilities.

### **PE-07: PHYSICAL ACCESS CONTROLS**

Agencies shall implement physical access controls at all physical access points, including designated entry/exit points, to agency facilities and secured areas within the facilities where information assets reside, excluding facility areas officially designated as publicly accessible. These physical access controls include:

- (a) Security perimeters (e.g. barriers such as walls, card controlled entry gates, or manned reception desks);
- (b) Validation of individual access authorization before access is granted (e.g. identity and authorization controls, security badges, biometrics, etc.);
- (c) Control of access to agency facilities and areas shall be restricted in accordance with an assessment of risk;

- (d) Secure keys, combinations, and other physical access devices shall be implemented to restrict access to only authorized personnel;
- (e) Inventory and review of physical access devices on an annual basis; and
- (f) Procedures that require the changing of combinations and keys when keys are lost, combinations are compromised, or certain individuals are transferred or terminated.

Supplemental Guidance: Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas.

## **PE-08: SECURITY MONITORING AND AUDITING OF PHYSICAL ACCESS**

As applicable to mitigate risks of unauthorized physical access to information assets and to ensure compliance with applicable policy, contractual, regulatory, and statutory requirements, agencies shall implement security monitoring technologies and systems.

Agency personnel assigned to publicly accessible facilities shall periodically review and audit the physical security of agency information assets located in publicly accessible areas to detect any signs of unauthorized access, tampering, destruction, or theft.

Supplemental Guidance: Examples of security monitoring technologies and systems include, but are not limited to, closed circuit video systems, alarms, and intrusion detection systems, card-controlled entry systems, etc. As permissible by law, agency security monitoring systems and authorized agency personnel may monitor, record, audit, review, and log any physical access to its facilities and areas within said facilities.

## **PE-09: RETENTION OF SECURITY LOGS AND VIDEO**

Agencies are required to develop processes to ensure all audit logs of badge access and video from closed circuit video cameras that document access to agency facilities are retained in accordance with applicable statutory, regulatory, contractual, and State policy requirements.

To allow for the auditing of physical access and/or the investigation of security incidents, the following minimum retention requirements shall be adhered to:

- (a) Audit logs of badge access and video from closed circuit video cameras that document access to agency facilities are to be retained for no less than ninety (90) days;
- (b) Audit logs of badge access and video from closed circuit video cameras that document access to restricted access zones, such as data centers, server rooms, and other such areas are to be retained for no less than one (1) year; and
- (c) Visitor sign-in/sign-out logs shall be retained for no less than one (1) year.

Supplemental Guidance: The retention requirements listed above represent the minimum necessary to allow for effective security, auditing, and investigation in the event of an incident. State data retention requirements, as well as other policy, statutory, regulatory, or contractual requirements may require longer retention periods. Agencies should review all statutory or

regulatory retention requirements applicable to their facilities and the information that is processed or stored within them.

## **PE-10: CLEAN DESK/CLEAN SCREEN REQUIREMENTS**

Sensitive information, whether in paper or electronic form, must be protected from unauthorized access and disclosure.

Supplemental Guidance: When sensitive information is to be left in an unattended location, it should be secured in file cabinets or other appropriate containers. During non-working hours, desks should be cleared to prevent unauthorized access and disclosure of sensitive information. To prevent unauthorized access to, or duplication and transmission of, sensitive information, documents containing such information should not be left unattended on printers, copiers, or fax machines.

## **PE-11: POWER EQUIPMENT AND POWER CABLING**

All agency facilities must protect the power equipment and power cabling for information assets from damage and destruction.

## **PE-12: EMERGENCY SHUTOFF**

All agency facilities must be able to shut off power to information assets or individual asset components in emergency situations. In addition, emergency shutoff switches or devices must be placed in clear and accessible areas to facilitate safe and easy access for personnel, while also being protected from unauthorized access.

## **PE-13: EMERGENCY POWER**

Short-term, uninterruptible power supplies to facilitate an orderly shutdown of information assets in the event of a primary power source loss should be implemented based on the criticality of the information asset and business operations.

Data centers and other critical facilities must include long-term alternative power sources (e.g. generators) to provide power in the event of a prolonged outage.

## **PE-14: EMERGENCY LIGHTING**

All agency facilities must employ and maintain automatic emergency lighting that activates in the event of a power outage or disruption, and that indicates emergency exits and evacuation routes within the facility.

## **PE-15: FIRE PROTECTION**

All agency facilities must employ and maintain appropriate fire suppression and detection devices/systems.

## **PE-16: TEMPERATURE AND HUMIDITY CONTROLS**

All agency facilities must maintain temperature and humidity levels within the facility where the information asset resides, at operational levels. In addition, temperature and humidity monitoring must be ongoing.

## **PE-17: WATER DAMAGE PROTECTION**

All agency data processing facilities and data centers must protect information assets from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

## **PE-18: ALTERNATE WORK SITE**

Agencies shall develop plans and procedures to maintain business and operations continuity from alternate work sites, should the primary work site become unavailable.

## **PE-19: DELIVERY AND REMOVAL OF INFORMATION ASSETS**

Agencies shall develop procedures for the delivery and removal of information assets to and from agency facilities.

- (a) Agency equipment, information, and/or software shall not be taken off-site without documented prior authorization; and
- (b) All Agency facilities must authorize, monitor, and control shipments and equipment removals from the facility and maintain records of those items.

## **PE-20: SECURING PORTABLE INFORMATION ASSETS**

Individuals who are provided with portable information assets including, but not limited to: laptop computers, tablets, smart phones, removable media, etc., shall be responsible for the physical security and condition of these information assets. When an information asset is allocated to an individual, the individual assumes temporary custodianship of the asset.

Agency information assets issued to employees and contractors shall remain the property of the agency.

At a minimum, users of agency portable information assets shall take the following physical security preventive measures:

- (a) Portable information assets shall not be left in view in an unattended vehicle;
- (b) Portable information assets shall not be left in an unattended vehicle (in or out of view) overnight;
- (c) Portable information assets displaying sensitive information should be positioned, whenever possible, so that the screen cannot be viewed by others;
- (d) When leaving a portable information asset unattended in a hotel room, users shall physically secure it with a cable lock and/or lock it in a safe or cabinet;

- (e) In vulnerable situations, i.e., public areas such as airport lounges and conference centers, the portable information assets shall never be left unattended;
- (f) Portable information assets shall, whenever permitted, be carried as hand luggage when traveling; and
- (g) All portable information assets (laptops, tablets, smart phones, removable media, etc.) that contain sensitive information shall be encrypted.

## **PE-21: DISPOSAL/TRANSFER OF INFORMATION ASSETS**

Information assets shall be disposed of, or reassigned, in a manner that does not compromise the security of the asset, and in accordance with the [Media Sanitization Standard](#) as documented herein.

## **REFERENCES**

The requirements established in the Physical and Environmental Security policies and standards have been derived from following:

- NIST SP 800-53r5 Physical and Environmental Policies and Procedures (PE); and
- NIST CSF Protect/Data Security (PR.DS), Detect/Security Continuous Monitoring (DE.CM).

---

# CONTINGENCY PLANNING (CP)

---

## CP-01: PURPOSE

The purpose of Contingency Planning is to minimize the risk of system and service unavailability due to a variety of disruptions by providing effective and efficient solutions to enhance system availability.

## KEY TERMS

**Recovery Point Objective (RPO)** - The point in time to which data must be recovered after an outage.

**Recovery Procedures** - Actions necessary to restore data files of an information system and computational capability after a system failure.

**Recovery Time Objective (RTO)** - The overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or critical business processes.

## CP-02: POLICY

Agency and NJOIT management are required to develop, implement, test, and maintain contingency plans to ensure continuity of operations for all information systems that deliver or support essential or critical functions on behalf of the State of New Jersey.

Supplemental Guidance: Contingency planning is an important aspect of risk management. Ensuring availability for critical and essential systems and components allows agencies to meet its mandates that are dictated by statute, executive order, policy, or contract, and to ensure delivery of vital government services. By [statute](#) and [executive order](#), NJOIT is responsible for the management of executive branch information technology and telecommunications infrastructure. Agencies are to develop contingency plans in concert with NJOIT. Defining availability and recoverability requirements, along with security and privacy controls, are requirements of the [NJOIT System Architecture Review](#) policy and process.

## CP-03: CONTINGENCY PLAN

Agency CIOs in coordination with NJOIT management shall develop contingency plans that:

- (a) Identify and document essential mission and business functions and the associated contingency requirements;
- (b) Identify critical system assets supporting essential mission and business functions;
- (c) Provide recovery objectives, restoration priorities, and metrics;
- (d) Address contingency roles, responsibilities, and emergency contact information;
- (e) Address maintaining essential missions and business functions in the event of information system disruption, compromise, or failure;

- (f) Address eventual, full information system restoration without deterioration of the related security safeguards;
- (g) Address resumption of essential missions and business functions within a time frame specified by the Agency CIO and based on mission needs, applicable laws and regulations, and applicable contracts and agreements with other State agencies or external organizations;
- (h) Identify and document critical information system assets supporting agency missions and business functions;
- (i) Develop a contingency plan for the system that:
  1. Identifies essential mission and business functions and associated contingency requirements;
  2. Provides recovery objectives, restoration priorities, and metrics;
  3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
  4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;
  5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;
  6. Addresses the sharing of contingency information; and
  7. Addresses the resumption of essential, critical mission, and business functions for the system within the agency-defined time period.
- (j) Is coordinated with continuity of operations, business continuity, incident response, and other relevant plans;
- (k) Is reviewed and approved by agency and NJOIT management;
- (l) Distribute copies of the contingency plan to agency-defined key contingency personnel and groups;
- (m) Coordinate contingency planning activities with incident handling activities;
- (n) Review the contingency plan for the system at least annually;
- (o) Update the contingency plan to address changes to the agency, system, or environment of operation and the problems encountered during contingency plan implementation, execution, or testing;
- (p) Communicate contingency plan changes to agency-defined key contingency personnel groups;
- (q) Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and
- (r) Protect the contingency plan from unauthorized disclosure and modification.

Supplemental Guidance: In accordance with the Organizational Security Policy, Agency CIOs in coordination with the NJOIT and the State CTO are responsible for disaster recovery planning and operations.

## **CP-04: CONTINGENCY TRAINING**

Agencies shall develop and periodically provide contingency training to agency personnel consistent with their assigned roles and responsibilities and the current system environment and technologies.

Supplemental Guidance: Contingency training provided by agencies is linked to the assigned roles and responsibilities of agency personnel to ensure that the appropriate content and level of detail is included in such training. For example, some individuals may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to establish systems at alternate processing and storage sites; and agency officials may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles or responsibilities reflects the specific continuity requirements in the contingency plan. Events that may precipitate an update to contingency training content include, but are not limited to, contingency plan testing or an actual contingency (lessons learned), assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. At the discretion of the agency, participation in a contingency plan test or exercise, including lessons learned sessions subsequent to the test or exercise, may satisfy contingency plan training requirements.

## **CP-05: CONTINGENCY PLAN TESTING**

Agencies are required to:

- (a) Test the contingency plan for the system at agency-defined intervals to determine the effectiveness of the plan and the readiness to execute the plan;
- (b) Coordinate the contingency plan test with other related plans including continuity of operations, business continuity, and incident response;
- (c) Review the contingency plan test results; and
- (d) Initiate corrective actions and update the plan as necessary.

Supplemental Guidance: Agency CIOs should coordinate contingency plan testing for each agency information system with all key stakeholders, including customers, and other State agencies, business partners, vendors, and service providers that provide support for or are responsible for implementing the plan.

## **CP-06: ALTERNATE STORAGE SITE**

As part of the contingency planning process, agencies in coordination with NJOIT shall:

- (a) Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and
- (b) Ensure that the alternate storage site provides controls equivalent to that of the primary site.

Supplemental Guidance: Alternate storage sites should be geographically distinct from primary storage sites and maintain duplicate copies of information and data if the primary storage site is not available. Similarly, alternate processing sites provide processing capability if the primary processing site is not available. Items covered by alternate storage site agreements include environmental conditions at the alternate sites, access rules for systems and facilities, physical and environmental protection requirements, and coordination of delivery and retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential mission and business functions despite compromise, failure, or disruption in organizational systems.

## **CP-07: ALTERNATE PROCESSING SITE**

As part of the contingency planning process, agencies in coordination with NJOIT shall:

- (a) Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of agency-defined system operations for essential mission and business functions within the agency-defined time period consistent with recovery time objectives and recovery point objectives when the primary processing capabilities are unavailable;
- (b) Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and
- (c) Provide controls at the alternate processing site that are equivalent to those at the primary site.

Supplemental Guidance: Similar to alternate storage sites, alternate processing sites are geographically distinct from primary processing sites and provide processing capability if the primary processing site is not available. The alternate processing capability may be addressed using a physical processing site or other alternatives, such as failover to a cloud-based service provider or other internally or externally provided processing service.

## **CP-08: TELECOMMUNICATIONS SERVICES**

As part of the contingency planning process, agencies in coordination with NJOIT shall:

- (a) Establish alternate telecommunications services, including necessary agreements to permit the resumption of agency-defined system operations for essential mission and business functions within the agency-defined time period when the primary

telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites;

- (b) Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives);
- (c) Request Telecommunications Service Priority for all telecommunications services used for readiness if the primary and/or alternate telecommunications services are provided by a common carrier; and
- (d) Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

Supplemental Guidance: Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential mission and business functions despite the loss of primary telecommunications services. Alternate telecommunications services include additional ground-based circuits or lines, network-based approaches to telecommunications, or the use of satellites.

Agencies should consider the potential mission or business impact in situations where telecommunications service providers are servicing other organizations with similar priority of service provisions. Telecommunications Service Priority (TSP) is a Federal Communications Commission (FCC) program that directs telecommunications service providers (e.g., wireline and wireless phone companies) to give preferential treatment to users enrolled in the program when they need to add new lines or have their lines restored following a disruption of service, regardless of the cause.

In certain circumstances, telecommunications service providers or services may share the same physical lines, which increases the vulnerability of a single failure point. It is important to have provider transparency for the actual physical transmission capability for telecommunication services.

## **CP-09: SYSTEM BACKUP**

Agencies shall:

- (a) Conduct backups, consistent with the agency's recovery time objectives and recovery point objectives of user-level and system-level information contained in agency information systems and agency information system documentation, including security-related documentation;
- (b) Protect the confidentiality, integrity, and availability of backup information, including the use of cryptographic mechanisms based on the sensitivity of the data and other considerations;
- (c) Test backup information at least annually to verify media reliability and information integrity; and
- (d) Document the results of the backup tests.

Supplemental Guidance: System-level information includes system state information, operating system software, middleware, application software, and licenses. User-level information includes information other than system-level information. Mechanisms employed to protect the integrity of system backups include digital signatures and cryptographic hashes. The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of backup information.

## **CP-10: SYSTEM RECOVERY AND RECONSTITUTION**

Agencies shall:

- (a) Provide for the recovery and reconstitution of agency information systems to a known state within agency-defined time periods, consistent with recovery time objectives and recovery point objectives, after a disruption, compromise, or failure; and
- (b) Implement transaction recovery for systems that are transaction-based.

Supplemental Guidance: Recovery is executing contingency plan activities to restore organizational mission and business functions. Reconstitution takes place following recovery and includes activities for returning systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities; recovery point, recovery time, and reconstitution objectives; and organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of interim system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored system capabilities, reestablishment of continuous monitoring activities, system reauthorization (if required), and activities to prepare the system and organization for future disruptions, breaches, compromises, or failures. Recovery and reconstitution capabilities can include automated mechanisms and manual procedures. Agencies establish recovery time objectives and recovery point objectives as part of contingency planning.

Transaction-based systems include database management systems and transaction processing systems. Mechanisms supporting transaction recovery include transaction rollback and transaction journaling.

## **REFERENCES**

The requirements established in the Contingency Planning policy and standards have been derived from the following:

- NIST SP 800-53 Contingency Planning (CP), Program Management (PM); and
- NIST CSF Recovery/Improvements (RE.IM), Recovery/Recovery Planning (RE.RP)

---

## INCIDENT RESPONSE (IR)

---

### IR-01: PURPOSE

The purpose of the Incident Response policies and standards is to establish a consistent and organized approach for preparing for, identifying, reporting, and managing information security and privacy incidents that may compromise the confidentiality, integrity, availability, and privacy of the State's information and information systems.

### KEY TERMS

**Incident** - An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

**Significant Cybersecurity Incident** - A significant cyber incident is defined as an event that is likely to cause, or is causing, harm to critical business functions and services across the public and/or private sectors by impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks; and/or threatens public safety, undermines public confidence, has a negative effect on the economy, or diminishes the security posture of the State of New Jersey.

### IR-02: POLICY

In coordination with State agencies, the NJCCIC shall develop and maintain an information security and privacy incident response capability in order to effectively respond to cybersecurity incidents.

### IR-03: REPORTING INFORMATION SECURITY AND PRIVACY INCIDENTS

All agency personnel who are provided authorized access to agency information assets are responsible for promptly reporting suspected or actual security and privacy incidents.

(a) Suspected information security incidents may be reported via the following channels:

- Immediate supervisor;
- Agency IT Service Desk;
- Agency CISO;
- Agency HR Representative;
- NJOIT Enterprise Service Desk – 1.800.622.4357; and/or
- NJCCIC Incident Reporting Hotline – 1.833.465.2245  
<https://www.cyber.nj.gov/cyber-incident>

- (b) Upon notification from a user of a suspected information security or privacy incident, the receiving entity will document the information provided and notify the agency CISO and/or agency privacy officer or their designees of the report; and
- (c) Agencies shall report all incidents to the New Jersey Cybersecurity Communications and Integration Cell for de-confliction, trending, and assistance in responding to an incident.

Any attempt to interfere with, prevent, obstruct, or dissuade a user in their efforts to report a suspected security or privacy incident is strictly prohibited and cause for disciplinary action, up to and including termination. Any form of retaliation against an individual reporting or investigating a security incident or violation is also prohibited.

## **IR-04: INCIDENT RESPONSE PLANNING**

The State Chief Information Security Officer (CISO) shall be responsible for the development, maintenance, and promulgation of a Statewide Information Security and Privacy Incident Response Plan. Agencies are responsible for incorporating the strategies included in the statewide plan into their respective agency incident response plans:

- (a) The Information Security and Privacy Incident Response Plans shall encompass strategies for incident response preparation; detection and analysis; containment, eradication, and recovery; and post-incident analysis, in accordance with the NIST Special Publication (SP) 800-61 Revision 2, [Computer Security Incident Handling Guide](#);
- (b) The plans shall define the roles and responsibilities of incident response team participants, the characterization of incidents, relationships to other policies and procedures, and reporting requirements;
- (c) The State CISO shall be responsible for the development of a statewide incident response training curriculum, including table-top or simulation exercises to aid agencies in effectively responding to incidents. Agency CISOs are responsible for training activities within their respective agencies; and
- (d) Agency Heads shall be responsible for the implementation of the Information Security and Privacy Incident Response Plan within their respective agencies, including the designation of an agency Information Security and Privacy Incident Response Team (IRT) and an individual with responsibility to act as the agency's IRT Coordinator for the agency.

## **IR-05: INCIDENT RESPONSE TRAINING**

Agencies in coordination with the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) shall:

- (a) Provide incident response training to system users consistent with assigned roles and responsibilities:
  - 1. Upon assuming an incident response role or responsibility or acquiring system access;
  - 2. When required by system changes; and
  - 3. At least annually thereafter;

- (b) Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach; and
- (c) Review and update incident response training content annually and following any significant cybersecurity incident.

Supplemental Guidance: Incident response training is associated with the assigned roles and responsibilities of agency personnel to ensure that the appropriate content and level of detail are included in such training. For example, users may only need to know who to call or how to recognize an incident; system administrators may require additional training on how to handle incidents; and incident responders may receive more specific training on forensics, data collection techniques, reporting, system recovery, and system restoration. Incident response training includes user training in identifying and reporting suspicious activities from external and internal sources. Training should include simulated events and tests or exercises of the agency's and the State's incident response capabilities.

## **IR-06: INCIDENT RESPONSE TESTING**

The NJCCIC in coordination with State agencies shall test the effectiveness of the State's incident response capabilities at least annually by creating checklists and playbooks, and conducting table-top exercises and simulations that include a variety of incidents, including data breaches.

Supplemental Guidance: Agencies should develop testing for individual information systems so that response personnel are familiar with their roles and responsibilities with respect to the specific information system.

## **IR-07: INCIDENT RESPONSE TEAM**

Agency CISOs shall establish an agency Information Security and Privacy Incident Response Team (IRT) that is charged with promptly and correctly handling information security incidents that may impact the agency, including its systems, networks, services, data, customers, and employees.

- (a) The IRT should be comprised of capable members from the agency IT team, agency information security team, agency privacy officer, the agency legal representative, the agency public information office, the agency human resources department, and auxiliary functions or resources, as necessary;
- (b) Agencies shall assign an IRT Coordinator who is responsible for coordinating the response of the agency IRT and for communicating or escalating the incident as appropriate;
- (c) The IRT is responsible for carrying out the agency's response to information security incidents;
- (d) The IRT is authorized to take the appropriate steps deemed necessary to contain, mitigate, and resolve an information security incident in an effective and efficient manner;
- (e) The IRT is authorized to take necessary action to protect agency information assets or preserve evidence;

- (f) The incident's classification, severity, and other factors will dictate which IRT members are required to respond to an incident. From the time an incident is reported to the IRT, members who have received the report are responsible for:
  - (1) Validating the initial report and declaring an incident as appropriate;
  - (2) Determining the type, severity, and priority of the incident; and
  - (3) Notifying the IRT Coordinator or an authorized designee of the incident;
- (g) The IRT Coordinator will determine which IRT members play an active role in the response and:
  - (1) Coordinate the agency's response efforts;
  - (2) Engage auxiliary agencies and resources as necessary;
  - (3) Escalate incidents to executive management as appropriate;
  - (4) Monitor progress of the response;
  - (5) Ensure evidence gathering, chain of custody, and preservation is appropriate;
  - (6) Manage all communications with outside organizations (i.e., law enforcement, media, and regulatory bodies);
  - (7) Manage all communications with external Agencies such as NJOIT and NJCCIC; and
  - (8) Prepare a written summary of the incident and corrective action taken.

Supplemental Guidance: The agency IRT Coordinator is typically the agency CIO or CISO. It should be an individual with the ability and authority to make decisions regarding the overall management of an information security incident. The IRT Coordinator must understand all facets of incident handling. The IRT is to be comprised of individuals with the skills and abilities to effectively handle and incident.

As necessary to effectively respond to an incident, the agency IRT will be supported by the New Jersey Cybersecurity and Communications Integration Cell and the New Jersey Office of Information Technology. For agencies that do not have the resources to handle information security incidents, the NJCCIC can provide incident response assistance. Depending on the nature and severity of the incident, the State CISO or his/her designee may assume the role of the IRT Coordinator.

## **IR-08: SIGNIFICANT CYBERSECURITY INCIDENTS**

Significant cybersecurity incidents may result in the activation of the State Emergency Operations Plan (SEOP). In such instances, the State will augment its incident response plan activities within the constructs of the Cyber Incident Annex to the SEOP. In accordance with [Executive Order 178](#) (Christie 2016), the NJCCIC may draw upon the assistance of any department, office, division, or agency of this State to supply it with expertise and assistance, including information and personnel, when responding to a cybersecurity incident.

## IR-09: INCIDENT CATEGORIZATION

To ensure a consistent approach to the reporting, response, handling, and tracking of incidents, agencies will use the following categorizations to describe the type of incident.

Category	Name	Description
Cat 0	Security Testing	This category is used during agency approved vulnerability and penetration testing activities and other security exercises intended to test the network defenses or responses.
Cat 1	Unauthorized Access	An individual gains logical or physical access, without authorization to an agency network, system, application, private or restricted data, or other information asset.
Cat 2	Denial of Service (DoS)	An attack that successfully prevents or impairs the normal authorized functionality of agency networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
Cat 3	Malicious Code	Successful installation of malicious software (e.g., virus, worm, Trojan horse, ransomware, or other code-based malicious entity) that infects an agency operating system or application.
Cat 4	Improper Usage	A user violates the Rules of Behavior - Acceptable Use of State Information Assets Policy or other agency or State policies.
Cat 5	Scans, Probes, Attempted Access	Any activity that seeks to access or identify an agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.
Cat 6	Investigation	Unconfirmed incidents that are potentially malicious, or anomalous activity, deemed by the reporting entity to warrant further review.
Cat 7	Data Breach	<p>A Data Breach is:</p> <ul style="list-style-type: none"> <li>• The compromise of the confidentiality of personally identifiable information;</li> <li>• The loss of data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of personally identifiable information;</li> <li>• Access to personally identifiable information that is for an unauthorized purpose; or</li> <li>• Access to personally identifiable information that is in excess of authorization.</li> </ul>

Incidents that may include activity spanning across multiple categories will be classified according to the category associated with the highest severity level.

## **IR-10: INCIDENT SEVERITY AND PRIORITIZATION**

Agencies shall classify the severity of the incidents using one of the following three (3) levels:

- (a) High;
- (b) Medium; or
- (c) Low.

Supplemental Guidance: The severity of an information security incident determines the priority and resources necessary to handle the incident. It also determines the timing and extent of the response, the documentation and communications. Severity is a subjective measure of the incident's impact on, or threat to, the confidentiality, integrity, availability, and privacy of agency information and information assets. An incident's severity level may be revised throughout the various incident response phases as dictated by information that is developed.

Agencies must consider the following factors when determining the severity of an incident:

- Threat to human safety;
- Scope of impact – number and criticality of systems, services, agencies, and people affected;
- Financial impact to the agency or State - loss of revenue, financial penalties, etc.;
- Sensitivity of the information – personally identifiable information (PII) or other sensitive information;
- Probability of propagation - likelihood that the malware or negative impact will spread or propagate to other systems or agencies;
- Reputational impact to the State or an individual agency; and
- Legal obligations and risks - notification requirements, regulatory issues, potential lawsuits, etc.

Other factors beyond those listed above may affect the severity rating of an incident.

## **IR-11: INCIDENT TRACKING, DOCUMENTATION, AND REPORTS**

Agencies shall establish procedures to ensure all incident response activities are documented to include artifacts and evidence obtained using methods consistent with chain of custody and confidentiality requirements.

- (a) Documents and artifacts associated with incidents shall be protected commensurate with their sensitivity and are to be protected from tampering;
- (b) Agencies shall establish processes for recording and maintaining incident reports;

- (c) The NJCCIC shall be responsible for developing and maintaining a centralized incident tracking system to aid in enhancing the response to incidents and their prevention; and
- (d) All agencies shall report all incidents to the NJCCIC for entry into the incident tracking system.

Supplemental Guidance: Individual security incidents may require completion of an incident report that provides a summary of the incident, its resolution, and any recommendations to help mitigate the risk of a reoccurrence.

## REFERENCES

The requirements established in the Incident Response policies and standards have been derived from the following:

- NIST SP 800-53r5 Incident Response (IR);
- NIST CSF Protect/Information Protection Processes and Procedures (PR.IP), Detect/Anomalies and Events (DE.AE), Respond/Response Planning (RS.RP), Respond/Analysis (RS.AN), Respond/Mitigate (RS.MI), Respond/Communications (RS.CO); and
- NIST Special Publication (SP) 800-61 Revision 2, [Computer Security Incident Handling Guide](#).

---

## APPENDIX A – GLOSSARY OF KEY TERMS

---

### **Acceptance:**

The point at which the end-users of a system declare, formally, that the system meets their needs and has performed satisfactorily during the test procedures. Unless a system has been acquired, installed, or amended, purely for IT department it is not sufficient for technical staff to declare it acceptable; the end users must be involved. (SOURCE: The Information Security Glossary)

### **Access (Logical):**

The process of being able to enter, modify, delete, or inspect, records and data held on a computer system by means of providing an ID and password (if required). The view that restricting physical access relieves the need for logical access restrictions is misleading. Any Agency with communications links to the outside world has a security risk of logical access. (SOURCE: The Information Security Glossary)

### **Access:**

Ability to make use of any information system (IS) resource. (SOURCE: NIST SP 800-32)

Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions. (SOURCE: CNSSI-4009)

### **Access Control:**

The process of granting or denying specific requests to:

1. obtain and use information and related information processing services; and
2. enter specific physical facilities (e.g., federal buildings, military establishments, and border crossing entrances). (SOURCE: FIPS 201; CNSSI-4009)

### **Access Control List (ACL):**

1. A list of permissions associated with an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object.
2. A mechanism that implements access control for a system resource by enumerating the system entities that are permitted to access the resource and stating, either implicitly or explicitly, the access modes granted to each entity. (SOURCE: CNSSI-4009)

### **Access Control Mechanism:**

Security safeguards (i.e., hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these) designed to detect and deny unauthorized access and permit authorized access to an information system. (SOURCE: CNSSI-4009)

**Access Level:**

A category within a given security classification limiting entry or system connectivity to only authorized persons. (SOURCE: CNSSI-4009)

**Access List:**

Roster of individuals authorized admittance to a controlled area. (SOURCE: CNSSI-4009)

**Access Management:**

A discipline that focuses on ensuring that only approved roles are able to create, read, update, or delete data – and only using appropriate and controlled methods. Data Governance programs often focus on supporting Access Management by aligning the requirements and constraints posed by Governance, Risk Management, Compliance, Security, and Privacy efforts. (SOURCE: Data Governance Institute)

**Access Point:**

A device that logically connects wireless client devices operating in infrastructure to one another and provides access to a distribution system, if connected, which is typically an organization's enterprise network. (SOURCE: NIST SP 800-48; NIST SP 800-121)

**Access Profile:**

Association of a user with a list of protected objects the user may access. (SOURCE: CNSSI-4009)

**Account Management, User:**

Involves:

1. the process of requesting, establishing, issuing, and closing user accounts;
2. tracking users and their respective access authorizations; and
3. managing these functions.

(SOURCE: NIST SP 800-12)

**Accountability:**

The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. (SOURCE: NIST SP 800-27)

Principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information. (SOURCE: CNSSI-4009)

**Activation Data:**

Private data, other than keys, that are required to access cryptographic modules.

(SOURCE: NIST SP 800-32)

**Active Attack:**

An attack that alters a system or data. (SOURCE: CNSSI-4009)

**Active Security Testing:**

Security testing that involves direct interaction with a target, such as sending packet to a target. (SOURCE: NIST SP 800-115)

**Ad Hoc Network:**

A wireless network that dynamically connects wireless client devices to each other without the use of an infrastructure device, such as an access point or a base station. (SOURCE: NIST SP 800-121)

**Add-on Security:**

Incorporation of new hardware, software, or firmware safeguards in an operational information system. (SOURCE: CNSSI-4009)

**Adequate Security:**

Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. (SOURCE: NIST SP 800-53; FIPS 200; OMB Circular A-130, App. III)

Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

Note: This includes assuring that information systems operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost effective management, personnel, operational, and technical controls.

(SOURCE: CNSSI-4009; NIST SP 800-37)

**Administrative Account:**

A user account with full privileges on a computer. (SOURCE: NIST SP 800-69)

**Administrative Safeguards:**

Administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic health information and to manage the conduct of the covered entity's workforce in relation to protecting that information. (SOURCE: NIST SP 800-66)

**Advanced Encryption Standard – (AES):**

The Advanced Encryption Standard specifies a U.S. government- approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. This standard specifies

the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. (SOURCE: FIPS 197)

A U.S. government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. (SOURCE: CNSSI-4009)

**Advanced Key Processor (AKP):**

A cryptographic device that performs all cryptographic functions for a management client node and contains the interfaces to

1. exchange information with a client platform,
2. interact with fill devices, and
3. connect a client platform securely to the primary services node (PRSN).

(SOURCE: CNSSI-4009)

**Advanced Persistent Threats (APT):**

An adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat:

- (i) pursues its objectives repeatedly over an extended period of time;
- (ii) adapts to defenders' efforts to resist it; and
- (iii) is determined to maintain the level of interaction needed to execute its objectives.

(SOURCE: NIST SP 800-39)

**Adversary:**

Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. (SOURCE: NIST SP 800-30)

**Advisory:**

Notification of significant new trends or developments regarding the threat to the information systems of an organization. This notification may include analytical insights into trends, intentions, technologies, or tactics of an adversary targeting information systems. (SOURCE: CNSSI-4009)

**Affordable Care Act:**

U.S. federal statute signed into law on March 23, 2010, with the goal of expanding public and private insurance coverage and reducing the cost of healthcare for individuals and the government. (SOURCE: IRS PUB 1075)

**Agency:**

The term “agency” is used to refer to any Department, Agency, Commission, Board, Body, or other instrumentality of the Executive Branch of New Jersey State Government.

**Agent:**

A program acting on behalf of a person or organization. (SOURCE: NIST SP 800-95)

**Alert:**

Notification that a specific attack has been directed at an organization’s information systems. (SOURCE: CNSSI-4009)

**Algorithm:**

A step-by-step procedure for calculations. Algorithms are used for calculation, data processing, and automated reasoning.

An algorithm is an effective method expressed as a finite list of well-defined instructions for calculating a function. Starting from an initial state and initial input (perhaps empty), the instructions describe a computation that, when executed, proceeds through a finite number of well-defined successive states, eventually producing "output" and terminating at a final ending state. The transition from one state to the next is not necessarily deterministic; some algorithms, known as randomized algorithms, incorporate random input. (SOURCE: WIKIPEDIA)

**All-Source Intelligence:**

Intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open-source data in the production of finished intelligence.

**Alternate Processing Site:**

Locations and infrastructures from which emergency or backup processes are executed, when the main premises are unavailable or destroyed. (SOURCE: ISACA)

**Analysis:**

The examination of acquired data for its significance and probative value to the case. (SOURCE: NIST SP 800-72)

**Anomaly-Based Detection:**

The process of comparing definitions of what activity is considered normal against observed events to identify significant deviations. (SOURCE: NIST SP 800-94)

**Anti-spoof:**

Countermeasures taken to prevent the unauthorized use of legitimate Identification & Authentication (I&A) data, however it was obtained, to mimic a subject different from the attacker. (SOURCE: CNSSI-4009)

**Anti-Virus Software:**

A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents. (SOURCE: NIST SP 800-83)

**Antispyware Software:**

A program that specializes in detecting both malware and non-malware forms of spyware. (SOURCE: NIST SP 800-69)

**Applicant:**

The subscriber is sometimes called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. (SOURCE: NIST SP 800-32)

**Application:**

A software program hosted by an information system. (SOURCE: NIST SP 800-37)

Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges. (SOURCE: CNSSI-4009)

**Application Program Interface (API):**

An API specifies how some software components should interact with each other. In addition to accessing databases or computer hardware, such as hard disk drives or video cards, an API can be used to ease the work of programming graphical user interface components. In practice, many times an API comes in the form of a library that includes specifications for routines, data structures, object classes, and variables. In some other cases, notably for SOAP and REST services, an API comes as just a specification of remote calls exposed to the API consumers. (SOURCE: WIKIPEDIA)

**Application Service Providers (ASPs):**

Companies that offer individuals or enterprises access over the Internet to applications and related services that would otherwise have to be located in their own personal or enterprise computers. Sometimes referred to as "apps-on-tap," ASP services are expected to become an important alternative, not only for smaller companies with low budgets for information technology, but also for larger companies as a form of outsourcing and for many services for individuals as well. Most corporations are essentially providing their own ASP service in-house, moving applications off personal computers, and putting them on a special kind of application server that is designed to handle the stripped-down kind of thin-client workstation. This allows an enterprise to reassert the central control over application cost and usage that corporations formerly had prior to the advent of the PC. (SOURCE: TechTarget)

**Approval to Operate (ATO):**

The official management decision issued by a DAA or PAA to authorize operation of an information system and to explicitly accept the residual risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. (SOURCE: CNSSI-4009)

**Approved Mode of Operation:**

A mode of the cryptographic module that employs only Approved security functions (not to be confused with a specific mode of an Approved security function, e.g., Data Encryption Standard Cipher- Block Chaining (DES CBC) mode). (SOURCE: FIPS 140-2)

**Approved Security Function:**

A security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either:

- a. specified in an Approved Standard;
- b. adopted in an Approved Standard and specified either in an appendix of the Approved Standard or in a document referenced by the Approved Standard; or
- c. specified in the list of Approved security functions. (SOURCE: FIPS 140-2)

**Assessment:**

See Security Control Assessment.

**Assessment Findings:**

Assessment results produced by the application of an assessment procedure to a security control or control enhancement to achieve an assessment objective; the execution of a determination statement within an assessment procedure by an assessor that results in either a satisfied or other than satisfied condition. (SOURCE: NIST SP 800-53A)

**Assessment Method:**

One of three types of actions (i.e., examine, interview, test) taken by assessors in obtaining evidence during an assessment. (SOURCE: NIST SP 800-53A)

**Assessment Object:**

The item (i.e., specifications, mechanisms, activities, individuals) upon which an assessment method is applied during an assessment. (SOURCE: NIST SP 800-53A)

**Assessment Procedure:**

A set of assessment objectives and an associated set of assessment methods and assessment objects. (SOURCE: NIST SP 800-53A)

**Assessor:**

See Security Control Assessor.

**Asset:**

See Information Asset.

**Asset Custodian:**

A person or group responsible for the day-to-day management, operation, and security of an asset. An asset custodian typically has a role of system, database, or network administrator. Asset custodian is synonymous with data or information custodian.

**Asset Identification:**

Security Content Automation Protocol (SCAP) constructs to uniquely identify assets (components) based on known identifiers and/or known information about the assets. (SOURCE: NIST SP 800-128)

**Asset Owner:**

A person or organizational unit (internal or external to the organization) with primary responsibility for the viability, productivity, security, and resilience of an organizational asset. For example, the accounts payable department is the owner of the vendor database. (SOURCE: CERT RMM)

**Asset Reporting Format (ARF):**

SCAP data model for expressing the transport format of information about assets (components) and the relationships between assets and reports. (SOURCE: NIST SP 800-128)

**Assurance:**

Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. "Adequately met" includes:

1. functionality that performs correctly,
2. sufficient protection against unintentional errors (by users or software), and
3. sufficient resistance to intentional penetration or by-pass.

(SOURCE: NIST SP 800-27)

The grounds for confidence that the set of intended security controls in an information system are effective in their application. (SOURCE: NIST SP 800-37; NIST SP 800-53A)

Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy. (SOURCE: CNSSI-4009; NIST SP 800-39)

In the context of OMB M-04-04 and this document, assurance is defined as:

1. the degree of confidence in the vetting process used to establish the identity of an individual to whom the credential was issued, and
2. the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued. (SOURCE: NIST SP 800-63)

**Assurance Case:**

A structured set of arguments and a body of evidence showing that an information system satisfies specific claims with respect to a given quality attribute. (SOURCE: NIST SP 800-53A; NIST SP 800-39)

**Assured Information Sharing:**

The ability to confidently share information with those who need it, when and where they need it, as determined by operational need and an acceptable level of security risk. (SOURCE: CNSSI-4009)

**Assured Software:**

Computer application that has been designed, developed, analyzed, and tested using processes, tools, and techniques that establish a level of confidence in it. (SOURCE: CNSSI-4009)

**Asymmetric Cryptography:**

See Public Key Cryptography. (SOURCE: CNSSI-4009)

**Asymmetric Keys:**

Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification. (SOURCE: FIPS 201)

**Asynchronous Transfer Mode (ATM):**

A telecommunications concept defined by ANSI and ITU standards for carriage of a complete range of user traffic, including voice, data, and video signals. (SOURCE: WIKIPEDIA)

**Attack:**

An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity. (SOURCE: NIST SP 800-32)

Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. (SOURCE: CNSSI-4009)

**Attack Sensing and Warning (AS&W):**

Detection, correlation, identification, and characterization of intentional unauthorized activity with notification to decision makers so that an appropriate response can be developed. (SOURCE: CNSSI-4009)

**Attack Signature:**

A specific sequence of events indicative of an unauthorized access attempt. (SOURCE: NIST SP 800-12)

A characteristic byte pattern used in malicious code or an indicator, or set of indicators, that allows the identification of malicious network activities. (SOURCE: CNSSI-4009)

**Attack Surface:**

The set of points on the boundary of a system, a system component, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, component, or environment.

**Attribute-Based Access Control:**

Access control based on attributes associated with and about subjects, objects, targets, initiators, resources, or the environment. An access control rule set defines the combination of attributes under which an access may take place. (SOURCE: NIST SP 800-53; CNSSI-4009)

**Attribute-Based Authorization:**

A structured process that determines when a user is authorized to access information, systems, or services based on attributes of the user and of the information, system, or service. (SOURCE: CNSSI-4009)

**Audit:**

Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. (SOURCE: NIST SP 800-32)

Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures. (SOURCE: CNSSI-4009)

**Audit Data:**

Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. (SOURCE: NIST SP 800-32)

**Audit Log:**

A chronological record of system activities. Includes records of system accesses and operations performed in a given period. (SOURCE: CNSSI-4009)

**Audit Reduction Tools:**

Preprocessors designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tools can remove many audit records known to have little security significance. These tools generally remove records generated by specified classes of events, such as records generated by nightly backups. (SOURCE: NIST SP 800-12; CNSSI-4009)

**Audit Review:**

The assessment of an information system to evaluate the adequacy of implemented security controls, assure that they are functioning properly, identify vulnerabilities, and assist in implementation of new security controls where required. This assessment is conducted annually or whenever significant change has occurred and may lead to recertification of the information system. (SOURCE: CNSSI-4009)

**Audit Trail:**

A record showing who has accessed an Information Technology (IT) system and what operations the user has performed during a given period. (SOURCE: NIST SP 800-47)

A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result. (SOURCE: CNSSI-4009)

**Authenticate:**

To confirm the identity of an entity when that identity is presented. (SOURCE: NIST SP 800-32)

To verify the identity of a user, user device, or other entity. (SOURCE: CNSSI-4009)

**Authentication:**

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. (SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-27; FIPS 200; NIST SP 800-30)

The process of establishing confidence of authenticity. (SOURCE: FIPS 201)

Encompasses identity verification, message origin authentication, and message content authentication. (SOURCE: FIPS 190)

A process that establishes the origin of information or determines an entity's identity. (SOURCE: NIST SP 800-21)

The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data. (SOURCE: CNSSI-4009)

The process of establishing confidence in the identity of users or information systems. (SOURCE: NIST SP 800-63)

**Authentication Code:**

A cryptographic checksum based on an Approved security function (also known as a Message Authentication Code [MAC]). (SOURCE: FIPS 140-2)

**Authentication Mechanism:**

Hardware-or software-based mechanisms that force users to prove their identity before accessing data on a device. (SOURCE: NIST SP 800-72; NIST SP 800-124)

Hardware or software-based mechanisms that forces users, devices, or processes to prove their identity before accessing data on an information system. (SOURCE: CNSSI-4009)

**Authentication Mode:**

A block cipher mode of operation that can provide assurance of the authenticity and, therefore, the integrity of data. (SOURCE: NIST SP 800-38B)

**Authentication Period:**

The maximum acceptable period between any initial authentication process and subsequent re-authentication processes during a single terminal session or during the period data is being accessed. (SOURCE: CNSSI-4009)

**Authentication Protocol:**

A defined sequence of messages between a Claimant and a Verifier that demonstrates that the Claimant has possession and control of a valid token to establish his/her identity, and optionally, demonstrates to the Claimant that he or she is communicating with the intended Verifier. (SOURCE: NIST SP 800-63)

A well-specified message exchange process between a claimant and a verifier that enables the verifier to confirm the claimant's identity. (SOURCE: CNSSI-4009)

**Authentication Tag:**

A pair of bit strings associated to data to provide assurance of its authenticity. (SOURCE: NIST SP 800-38B)

**Authentication Token:**

Authentication information conveyed during an authentication exchange. (SOURCE: FIPS 196)

**Authenticator:**

The means used to confirm the identity of a user, process, or device (e.g., user password or token). (SOURCE: NIST SP 800-53; CNSSI-4009)

**Authenticity:**

The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication. (SOURCE: NIST SP 800-53; NIST SP 800-53A; CNSSI-4009; NIST SP 800-39)

**Authority:**

Person(s) or established bodies with rights and responsibilities to exert control in an administrative sphere. (SOURCE: CNSSI-4009)

**Authorization:**

Access privileges granted to a user, program, or process or the act of granting those privileges. (SOURCE: CNSSI-4009)

**Authorization Boundary:**

All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected. (SOURCE: CNSSI-4009; NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37)

**Automated Key Transport:**

The transport of cryptographic keys, usually in encrypted form, using electronic means such as a computer network (e.g., key transport/agreement protocols). (SOURCE: FIPS 140-2)

**Automated Security Monitoring:**

Use of automated procedures to ensure security controls are not circumvented or the use of these tools to track actions taken by subjects suspected of misusing the information system. (SOURCE: CNSSI-4009)

**Autonomous System (AS):**

One or more routers under a single administration operating the same routing policy. (SOURCE: NIST SP 800-54)

**Availability:**

In the context of information security, refers to ensuring timely and reliable access to and use of information. The loss of availability is the disruption of access to or use of information or an information system. [44 U.S.C., Sec. 3542]

Ensuring timely and reliable access to and use of information.

(SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-27; NIST SP 800-60; NIST SP 800-37; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542)

The property of being accessible and useable upon demand by an authorized entity.

(SOURCE: CNSSI-4009)

**Awareness (Information Security):**

Activities which seek to focus an individual's attention on an (information security) issue or set of issues. (SOURCE: NIST SP 800-50)

**Backdoor:**

Typically unauthorized hidden software or hardware mechanism used to circumvent security controls. (SOURCE: CNSSI-4009)

An undocumented way of gaining access to a computer system. A backdoor is a potential security risk. (SOURCE: NIST SP 800-82)

**Bandwidth:**

Commonly used to mean the capacity of a communication channel to pass data through the channel in a given amount of time. Usually expressed in bits per second. (SOURCE: Safety Engineering: Principles and Practices)

**Banner:**

The information that is displayed to a remote user trying to connect to a service. This may include version information, system information, or a warning about authorized use. (SOURCE: Intrusion Detection Systems)

**Banner Grabbing:**

The process of capturing banner information—such as application type and version—that is transmitted by a remote port when a connection is initiated. (SOURCE: NIST SP 800-115)

**Baseline:**

Hardware, software, databases, and relevant documentation for an information system at a given point in time. (SOURCE: CNSSI-4009)

**Baseline Assessment:**

An interim compliance validation assessment performed by a QSA to determine the PCI Security compliance status. (SOURCE: VERIZON PCI SECURITY)

**Baseline Configuration:**

A set of specifications for a system, or Configuration Item (CI) within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes. (SOURCE: NIST SP 800-128)

**Baseline Security:**

The minimum security controls required for safeguarding an IT system based on its identified needs for confidentiality, integrity, and/or availability protection. (SOURCE: NIST SP 800-16)

**Baselining:**

Monitoring resources to determine typical utilization patterns so that significant deviations can be detected. (SOURCE: NIST SP 800-61)

**Basic Testing:**

A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Also known as black box testing. (SOURCE: NIST SP 800-53A)

**Bastion Host:**

A special-purpose computer on a network specifically designed and configured to withstand attacks. (SOURCE: CNSSI-4009)

**Best Practice:**

A proven activity or process that has been successfully used by multiple enterprises. (SOURCE: ISACA)

**Binding:**

Process of associating two related elements of information. (SOURCE: NIST SP 800-32)

An acknowledgement by a trusted third party that associates an entity's identity with its public key. This may take place through:

1. a certification authority's generation of a public key certificate,
2. a security officer's verification of an entity's credentials and placement of the entity's public key and identifier in a secure database, or
3. an analogous method.

(SOURCE: NIST SP 800-21)

Process of associating a specific communications terminal with a specific cryptographic key or associating two related elements of information. (SOURCE: CNSSI-4009)

**Biometric:**

A physical or behavioral characteristic of a human being. (SOURCE: NIST SP 800-32)

A measurable physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics. (SOURCE: FIPS 201)

**Biometric Information:**

The stored electronic information pertaining to a biometric. This information can be in terms of raw or compressed pixels or in terms of some characteristic (e.g., patterns.) (SOURCE: FIPS 201)

**Biometric System:**

An automated system capable of: 1) capturing a biometric sample from an end user; 2) extracting biometric data from that sample; 3) comparing the extracted biometric data with data contained in one or more references; 4) deciding how well they match; and 5) indicating whether or not an identification or verification of identity has been achieved.

(SOURCE: FIPS 201)

**Biometrics:**

Measurable physical characteristics or personal behavioral traits used to identify, or verify the claimed identity, of an individual. Facial images, fingerprints, and handwriting samples are all examples of biometrics. (SOURCE: CNSSI-4009)

**Black Box Testing:**

See Basic Testing.

**Blacklist:**

A list of email senders who have previously sent spam to a user. (SOURCE: NIST SP 800-114)

A list of discrete entities, such as hosts or applications that have been previously determined to be associated with malicious activity. (SOURCE: NIST SP 800-94)

**Blacklisting:**

The process of the system invalidating a user ID based on the user's inappropriate actions. A blacklisted user ID cannot be used to log on to the system, even with the correct authenticator. Blacklisting and lifting of a blacklisting are both security-relevant events. Blacklisting also applies to blocks placed against IP addresses to prevent inappropriate or unauthorized use of Internet resources. (SOURCE: CNSSI-4009)

**Blended Attack:**

A hostile action to spread malicious code via multiple methods. (SOURCE: CNSSI-4009)

**Blinding:**

Generating network traffic that is likely to trigger many alerts in a short period of time, to conceal alerts triggered by a "real" attack performed simultaneously. (SOURCE: NIST SP 800-94)

**Block:**

Sequence of binary bits that comprise the input, output, State, and Round Key. The length of a sequence is the number of bits it contains. Blocks are also interpreted as arrays of bytes. (SOURCE: FIPS 197)

**Block Cipher:**

A symmetric key cryptographic algorithm that transforms a block of information at a time using a cryptographic key. For a block cipher algorithm, the length of the input block is the same as the length of the output block. (SOURCE: NIST SP 800-90)

**Block Cipher Algorithm:**

A family of functions and their inverses that is parameterized by a cryptographic key; the function maps bit strings of a fixed length to bit strings of the same length. (SOURCE: NIST SP 800-67)

**Blog:**

A discussion or informational site published on the World Wide Web and consisting of discrete entries ("posts") typically displayed in reverse chronological order (the most recent post appears first). Blogs may be the work of a single individual, occasionally of a small group, and covering a single subject, or may include posts written by large numbers of authors and professionally edited. (SOURCE: WIKIPEDIA)

**Body of Evidence (BoE):**

The set of data that documents the information system's adherence to the security controls applied. The BoE will include a Requirements Verification Traceability Matrix (RVTM) delineating

where the selected security controls are met and evidence to that fact can be found. The BoE content required by an Authorizing Official will be adjusted according to the impact levels selected. (SOURCE: CNSSI-4009)

**Border Gateway Protocol (BGP):**

A standardized exterior gateway protocol designed to exchange routing and reachability information between autonomous systems (AS) on the Internet. The protocol is often classified as a path vector protocol, but is sometimes also classed as a distance vector routing protocol. The Border Gateway Protocol does not use Interior Gateway Protocol (IGP) metrics, but makes routing decisions based on paths, network policies and/or rule-sets configured by a network administrator. The Border Gateway Protocol plays a key role in the overall operation of the Internet and is involved in making core routing decisions. (SOURCE: WIKIPEDIA)

**Boundary Protection:**

Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communication, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels). (SOURCE: NIST SP 800-53; CNSSI-4009)

**Boundary Protection Device:**

A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) provides information system boundary protection. (SOURCE: NIST SP 800-53)

A device with appropriate mechanisms that facilitates the adjudication of different security policies for interconnected systems. (SOURCE: CNSSI-4009)

**Breach:**

The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for another than authorized purpose. (SOURCE: US OMB M-17-12)

An impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and

4. The extent to which the risk to the protected health information has been mitigated.  
(SOURCE: HIPAA (45 CFR §§ 164.400-414))

**Breach of Security:**

"Breach of security" means unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable. Good faith acquisition of personal information by an employee or agent of the business for a legitimate business purpose is not a breach of security, provided that the personal information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure.  
(SOURCE: N.J.S.A 2C.56:8-161)

**Bring Your Own Device (BYOD):**

Refers to the policy of permitting employees and contractors to use personally owned or third-party owned mobile devices (e.g. tablets, and smart phones) for State business purposes.  
(SOURCE: State of New Jersey Statewide Information Security Manual)

**Brute Force Password Attack:**

A method of accessing an obstructed device through attempting multiple combinations of numeric and/or alphanumeric passwords. (SOURCE: NIST SP 800-72)

**Buffer Overflow:**

A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system. (SOURCE: NIST SP 800-28; CNSSI-4009)

**Bulk Encryption:**

Simultaneous encryption of all channels of a multichannel telecommunications link.  
(SOURCE: CNSSI-4009)

**Business Associate:**

A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. (SOURCE: US Department of Health and Human Services)

**Business Continuity Plan (BCP):**

The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption. (SOURCE: NIST SP 800-34; CNSSI-4009)

**Business Entity:**

All trusted Entities that are authorized and/or contracted with a Department and/or Agency within the Executive Branch of State Government for the purpose of this policy Business Entity may include other governmental agencies outside the Executive Branch that do not make use of the Garden State Network. (SOURCE: NJOIT Glossary)

**Business Impact Analysis (BIA):**

An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. (SOURCE: NIST SP 800-34)

An analysis of an enterprise's requirements, processes, and interdependencies used to characterize information system contingency requirements and priorities in the event of a significant disruption. (SOURCE: CNSSI-4009)

**Call Back:**

Procedure for identifying and authenticating a remote information system terminal, whereby the host system disconnects the terminal and reestablishes contact. (SOURCE: CNSSI-4009)

**Card Skimmer:**

A physical device, often attached to a legitimate card-reading device, designed to illegitimately capture and/or store the information from a payment card. (SOURCE: PCI DSS GLOSSARY)

**Card Verification Value (CVV/CVV2):**

Both of these terms are commonly used to refer to the number printed on a card to help secure "card not present" transactions - other terms include CVC, CID and CSC. To be precise, the code printed on the card is actually the CVV2 - and the CVV is integrity-check data encoded on the magnetic strip - but both terms are widely used online. (SOURCE: VERIZON PCI SECURITY)

**Cardholder:**

An individual possessing an issued Personal Identity Verification (PIV) card. (SOURCE: FIPS 201)

**Cardholder Data Environment (CDE):**

All people, processes and technologies that store, process or transmit cardholder data (CHD) or sensitive authentication data (SAD). (SOURCE: VERIZON PCI SECURITY)

**Carrier Sense Multiple Access with Collision Detection (CSMA/CD):**

A media access control method used most notably in local area networking. It uses a carrier sensing scheme in which a transmitting data station detects other signals while transmitting a frame, and stops transmitting that frame, transmits a jam signal, and then waits for a random time interval before trying to resend the frame. (SOURCE: WIKIPEDIA)

**Category:**

Restrictive label applied to classified or unclassified information to limit access. (SOURCE: CNSSI-4009)

**Center for Internet Security (CIS) Benchmarks:**

CIS benchmarks are configuration baselines and best practices for securely configuring a system.

**Central Management:**

The organization-wide management and implementation of selected security and privacy controls and related processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed security and privacy controls and processes. (SOURCE: NIST 800-53r5)

**Certificate:**

A digital representation of information which at least

1. identifies the certification authority issuing it,
2. names or identifies its subscriber,
3. contains the subscriber's public key,
4. identifies its operational period, and
5. is digitally signed by the certification authority issuing it.

(SOURCE: NIST SP 800-32)

A set of data that uniquely identifies an entity, contains the entity's public key and possibly other information, and is digitally signed by a trusted party, thereby binding the public key to the entity. Additional information in the certificate could specify how the key is used and its crypto period. (SOURCE: NIST SP 800-21)

A set of data that uniquely identifies a key pair and an owner that is authorized to use the key pair. The certificate contains the owner's public key and possibly other information, and is digitally signed by a Certification Authority (i.e., a trusted party), thereby binding the public key to the owner. (SOURCE: FIPS 186)

**Certificate Management:**

Process whereby certificates (as defined above) are generated, stored, protected, transferred, loaded, used, and destroyed. (SOURCE: CNSSI-4009)

**Certificate Management Authority – (CMA):**

A Certification Authority (CA) or a Registration Authority (RA). (SOURCE: NIST SP 800-32)

**Certificate of Authority:**

In cryptography, a certificate authority or certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. A CA acts as a trusted third

party—trusted both by the subject (owner) of the certificate and by the party relying upon the certificate. The format of these certificates is specified by the X.509 standard. (SOURCE: Wikipedia)

**Certificate Policy (CP):**

A specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery, and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications. (SOURCE: CNSSI-4009; NIST SP 800-32)

**Certificate Revocation List (CRL):**

A list of revoked public key certificates created and digitally signed by a Certification Authority. (SOURCE: NIST SP 800-63; FIPS 201)

**Certification:**

A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (SOURCE: FIPS 200)

The process of verifying the correctness of a statement or claim and issuing a certificate as to its correctness. (SOURCE: FIPS 201)

Comprehensive evaluation of the technical and nontechnical security safeguards of an information system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements. See Security Control Assessment. (SOURCE: CNSSI-4009)

**Certification Authority (CA):**

A trusted entity that issues and revokes public key certificates. (SOURCE: FIPS 201)

The entity in a public key infrastructure (PKI) that is responsible for issuing certificates and exacting compliance to a PKI policy. (SOURCE: NIST SP 800-21; FIPS 186)

**Certification Authority Facility:**

The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation. (SOURCE: NIST SP 800-32)

**Certification Package:**

Product of the certification effort documenting the detailed results of the certification activities. (SOURCE: CNSSI-4009)

**Chain of Custody:**

A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer. (SOURCE: NIST SP 800-72; CNSSI-4009)

**Chain of Evidence:**

A process and record that shows who obtained the evidence; where and when the evidence was obtained; who secured the evidence; and who had control or possession of the evidence. The "sequencing" of the chain of evidence follows this order: collection and identification; analysis; storage; preservation; presentation in court; return to owner. (SOURCE: CNSSI-4009)

**Change:**

The addition, modification or removal of anything that could have an effect on IT services. The scope should include changes to all architectures, processes, tools, metrics and documentation, as well as changes to IT services and other configuration items. (SOURCE: ITIL V3)

**Change Control:**

A formal process used to ensure that a process, product, service, or technology component is modified only in accordance with agreed-upon rules. Many organizations have formal Change Control Boards that review and approve proposed modifications to technology infrastructures, systems, and applications. Data Governance programs often strive to extend the scope of change control to include additions, modifications, or deletions to data models and values for reference/master data. (SOURCE: Data Governance Institute)

**Change Control Board (CCB):**

A committee that makes decisions regarding whether or not proposed changes to a software project should be implemented. In short any changes to the Baseline Requirements agreed with the client, should be taken up by project team on approval from this committee. If any change is agreed by the committee, it is communicated to the project team and client and the requirement is Baselined with the change. The change control board is constituted of project stakeholders or their representatives. The authority of the change control board may vary from project to project, but decisions reached by the change control board are often accepted as final and binding. The decision of acceptance of the changes also depends upon the stage or phase of the project. The main objective is to ensure acceptance of the project (deliverable) by the client. (SOURCE: WIKIPEDIA)

**Check Word:**

Cipher text generated by cryptographic logic to detect failures in cryptography. (SOURCE: CNSSI-4009)

**Checksum:**

Value computed on data to detect error or manipulation. (SOURCE: CNSI-4009)

**Cipher:**

Series of transformations that converts plaintext to ciphertext using the Cipher Key. (SOURCE: FIPS 197)

Any cryptographic system in which arbitrary symbols or groups of symbols, represent units of plain text, or in which units of plain text are rearranged, or both. (SOURCE: CNSI-4009)

**Cipher Block Chaining-Message Authentication Code – (CBC-MAC):**

A secret-key block-cipher algorithm used to encrypt data and to generate a Message Authentication Code (MAC) to provide assurance that the payload and the associated data are authentic. (SOURCE: NIST SP 800-38C)

**Cipher Suite:**

Negotiated algorithm identifiers. Cipher suites are identified in human-readable form using a mnemonic code. (SOURCE: NIST SP 800-52)

**Cipher Text Auto-Key (CTAK):**

Cryptographic logic that uses previous cipher text to generate a key stream. (SOURCE: CNSI-4009)

**Ciphertext:**

Data output from the Cipher or input to the Inverse Cipher. (SOURCE: FIPS 197)

Data in its enciphered form. (SOURCE: NIST SP 800-56B)

**Claimant:**

A party whose identity is to be verified using an authentication protocol. (SOURCE: NIST SP 800-63; FIPS 201)

An entity that is or represents a principal for the purposes of authentication, together with the functions involved in an authentication exchange on behalf of that entity. A claimant acting on behalf of a principal must include the functions necessary for engaging in an authentication exchange. (e.g., a smartcard [claimant] can act on behalf of a human user [principal]). (SOURCE: FIPS 196)

An entity (user, device or process) whose assertion is to be verified using an authentication protocol. (SOURCE: CNSI-4009)

**Clear:**

To use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a

file(s) (e.g., file allocation table) but also may include all addressable locations. See comments on Clear/Purge Convergence. (SOURCE: NIST SP 800-88)

**Clear Text:**

Information that is not encrypted. (SOURCE: NIST SP 800-82)

**Clearing:**

Removal of data from an information system, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using common system capabilities (i.e., through the keyboard); however, the data may be reconstructed using laboratory methods. (SOURCE: CNSSI-4009)

**Client:**

A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a server. (SOURCE: NIST SP 800-32)

**Closed Security Environment:**

Environment providing sufficient assurance that applications and equipment are protected against the introduction of malicious logic during an information system life cycle. Closed security is based upon a system's developers, operators, and maintenance personnel having sufficient clearances, authorization, and configuration control. (SOURCE: CNSSI-4009)

**Cloud Access Security Broker (CASB):**

On-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement. Example security policies include authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, malware detection/prevention. (SOURCE: Gartner)

**Cloud Computing:**

A model for enabling on-demand network access to a shared pool of configurable IT capabilities/resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. This cloud model is composed of five essential characteristics (on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service); three service delivery models (Cloud Software as a Service [SaaS], Cloud Platform as a Service [PaaS], and Cloud Infrastructure as a Service [IaaS]); and four models for enterprise access (Private cloud, Community cloud, Public cloud, and Hybrid cloud).

Note: Both the user's data and essential security services may reside in and be managed within the network cloud. (SOURCE: CNSSI-4009)

**CloudConnect:**

A bundled offering of cloud-based Microsoft Office365 products, including email, instant messaging, video conferencing, file sharing, and storage. It enables user-friendly interagency communication and file sharing, multi-device content synchronization, and two-factor authenticated remote access. (SOURCE: State of New Jersey Statewide Information Security Manual)

**Cloud Service Provider:**

An entity that offers cloud-based platform, infrastructure, application, or storage services. Cloud service providers include internal entities, such as NJOIT, and external entities, such as Amazon, Microsoft, Salesforce, Google, and others. (SOURCE: State of New Jersey Statewide Information Security Manual)

**Cold Site:**

Backup site that can be up and operational in a relatively short time span, such as a day or two. Provision of services, such as telephone lines and power, is taken care of, and the basic office furniture might be in place, but there is unlikely to be any computer equipment, even though the building might well have a network infrastructure and a room ready to act as a server room. In most cases, cold sites provide the physical location and basic services. (SOURCE: CNSSI-4009)

A backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternate site. (SOURCE: NIST SP 800-34)

**Cold Start:**

Procedure for initially keying crypto-equipment.(SOURCE: CNSSI-4009)

**Collision:**

Two or more distinct inputs produce the same output. Also see Hash Function. (SOURCE: NIST SP 800-57 Part 1)

**Comingling:**

The presence of FTI and non-FTI data together on the same paper or electronic media. (SOURCE: IRS PUB 1075)

**Common Configuration Enumeration (CCE):**

A SCAP specification that provides unique, common identifiers for configuration settings found in a wide variety of hardware and software products. (SOURCE: NIST SP 800-128)

**Common Configuration Scoring System (CCSS):**

A set of measures of the severity of software security configuration issues. (SOURCE: NISTIR 7502)

A SCAP specification for measuring the severity of software security configuration issues. (SOURCE: NIST SP 800-128)

**Common Platform Enumeration (CPE):**

A SCAP specification that provides a standard naming convention for operating systems, hardware, and applications for the purpose of providing consistent, easily parsed names that can be shared by multiple parties and solutions to refer to the same specific platform type. (SOURCE: NIST SP 800-128)

**Common Vulnerabilities and Exposures (CVE):**

A dictionary of common names for publicly known information system vulnerabilities. (SOURCE: NIST SP 800-51; CNSSI-4009)

An SCAP specification that provides unique, common names for publicly known information system vulnerabilities. (SOURCE: NIST SP 800-128)

**Common Vulnerability Scoring System (CVSS):**

An SCAP specification for communicating the characteristics of vulnerabilities and measuring their relative severity. (SOURCE: NIST SP 800-128)

**Communications Security (COMSEC):**

A component of Information Assurance that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes crypto security, transmission security, emissions security, and physical security of COMSEC material. (SOURCE: CNSSI-4009)

**Comparison:**

The process of comparing a biometric with a previously stored reference. (SOURCE: FIPS 201)

**Compensating Security Control:**

A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system. (SOURCE: CNSSI-4009)

**Compliance:**

A discipline, set of practices, and/or organizational group that deals with adhering to laws, regulations, standards, and contractual arrangements. Also, the adherence to requirements. Data Governance programs often support many types of compliance requirements: Regulatory compliance, contractual compliance, adherence to internal standards, policies, and architectures, and conformance to rules for data management, project management, and other disciplines. (SOURCE: Data Governance Institute)

**Comprehensive Testing:**

A test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. Also known as white box testing.

(SOURCE: NIST SP 800-53A)

**Compromise:**

Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. (SOURCE: NIST SP 800-32; CNSSI-4009)

The unauthorized disclosure, modification, substitution, or use of sensitive data (including plaintext cryptographic keys and other CSPs). (SOURCE: FIPS 140-2)

**Component:**

A discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents a building block of an information system. Information system components include commercial information technology products. Also referred to as a system component. (SOURCE: NIST SP 800-53r4)

**Computer-Based Training:**

Computer-based training (CBT) is any course of instruction whose primary means of delivery is a computer. A CBT course (sometimes called courseware) may be delivered via a software product installed on a single computer, through a corporate or educational intranet, or over the Internet as Web-based training (SOURCE: TechTarget)

**Computer Cryptography:**

Use of a crypto-algorithm program by a computer to authenticate or encrypt/decrypt information. (SOURCE: CNSSI-4009)

**Computer Emergency Response Team (CERT):**

Acronym for Carnegie Mellon University's "Computer Emergency Response Team." The CERT Program develops and promotes the use of appropriate technology and systems management practices to resist attacks on networked systems, to limit damage, and to ensure continuity of critical services. (SOURCE: PCI DSS Glossary)

**Computer Incident Response Team (CIRT):**

Group of individuals usually consisting of Security Analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents. Also called a Computer Security Incident Response Team (CSIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability, or Cyber Incident Response Team). (SOURCE: CNSSI-4009)

**Computer Network Attack (CNA):**

Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (SOURCE: CNSSI-4009)

**Computer Network Defense (CND):**

Actions taken to defend against unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities. (SOURCE: CNSSI-4009)

**Computer Network Exploitation (CNE):**

Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary information systems or networks. (SOURCE: CNSSI-4009)

**Computer Security (COMPUSEC):**

Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated. (SOURCE: CNSSI-4009)

**Computer Security Incident:**

See incident.

**Computer Security Incident Response Team (CSIRT):**

A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability). (SOURCE: NIST SP 800-61)

**Computer Security Object (CSO):**

A resource, tool, or mechanism used to maintain a condition of security in a computerized environment. These objects are defined in terms of attributes they possess, operations they perform or are performed on them, and their relationship with other objects. (SOURCE: FIPS 188; CNSSI-4009)

**Computer Security Objects Register:**

A resource, tool, or mechanism used to maintain a condition of security in a computerized environment. These objects are defined in terms of attributes they possess, operations they perform or are performed on them, and their relationship with other objects. (SOURCE: FIPS 188; CNSSI-4009)

**Computer Security Objects Register:**

A collection of Computer Security Object names and definitions kept by a registration authority. (SOURCE: FIPS 188; CNSSI-4009)

**Confidentiality:**

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-18; NIST SP 800-27; NIST SP 800-60; NIST SP 800-37; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542)

The property that sensitive information is not disclosed to unauthorized individuals, entities, or processes. (SOURCE: FIPS 140-2)

The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information. (SOURCE: CNSSI-4009)

**Configuration Control:**

Process of controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modification prior to, during, and after system implementation. (SOURCE: CNSSI-4009; NIST SP 800-37; NIST SP 800-53)

**Configuration Item:**

Any component or other service asset that needs to be managed in order to deliver an IT service. (SOURCE: ITIL V3)

**Configuration Management:**

A structured process of managing and controlling changes to hardware, software, firmware, communications, and documentation throughout the system development life cycle. (SOURCE: IRS PUB 1075)

**Container:**

The file used by a virtual disk encryption technology to encompass and protect other files. (SOURCE: NIST SP 800-111)

**Contamination:**

Type of incident involving the introduction of data of one security classification or security category into data of a lower security classification or different security category. (SOURCE: CNSSI-4009)

**Content Filtering:**

The process of monitoring communications such as email and Web pages, analyzing them for suspicious content, and preventing the delivery of suspicious content to users. (SOURCE: NIST SP 800-114)

**Contingency Plan:**

Management policy and procedures used to guide an enterprise response to a perceived loss of mission capability. The Contingency Plan is the first plan used by the enterprise risk managers to

determine what happened, why, and what to do. It may point to the Continuity of Operations Plan (COOP) or Disaster Recovery Plan for major disruptions. (SOURCE: CNSSI-4009)

**Continuity of Operations (COOP) Plan:**

A predetermined set of instructions or procedures that describe how an organization’s mission essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations. (SOURCE: NIST SP 800-34)

Management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. The COOP is the third plan needed by the enterprise risk managers and is used when the enterprise must recover (often at an alternate site) for a specified period of time. Defines the activities of individual departments and agencies and their sub-components to ensure that their essential functions are performed. This includes plans and procedures that delineate essential functions; specifies succession to office and the emergency delegation of authority; provide for the safekeeping of vital records and databases; identify alternate operating facilities; provide for interoperable communications, and validate the capability through tests, training, and exercises. See also Disaster Recovery Plan and Contingency Plan. (SOURCE: CNSSI-4009)

**Continuous Monitoring:**

The process implemented to maintain a current security status for one or more information systems or for the entire suite of information systems on which the operational mission of the enterprise depends. The process includes:

1. The development of a strategy to regularly evaluate selected IA controls/metrics,
2. Recording and evaluating IA relevant events and the effectiveness of the enterprise in dealing with those events,
3. Recording changes to IA controls, or changes that affect IA risks, and
4. Publishing the current security status to enable information-sharing decisions involving the enterprise.

(SOURCE: CNSSI-4009)

Maintaining ongoing awareness to support organizational risk decisions. (SOURCE: NIST SP 800-137)

**Control:**

A means of managing a risk or ensuring that an objective is achieved. Controls can be preventative, detective, or corrective and can be fully automated, procedural, or technology-assisted human-initiated activities. They can include actions, devices, procedures, techniques, or other measures. (SOURCE: Data Governance Institute)

**Control Information:**

Information that is entered into a cryptographic module for the purposes of directing the operation of the module. (SOURCE: FIPS 140-2)

**Controlled Access Area:**

Physical area (e.g., building, room, etc.) to which only authorized personnel are granted unrestricted access. All other personnel are either escorted by authorized personnel or are under continuous surveillance. (SOURCE: CNSSI-4009)

**Controlled Area:**

Any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. (SOURCE: NIST SP 800-53)

**Controlled Interface:**

A boundary with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information systems. (SOURCE: CNSSI-4009; NIST SP 800-37)

**Cookie:**

A piece of state information supplied by a Web server to a browser, in a response for a requested resource, for the browser to store temporarily and return to the server on any subsequent visits or requests. (SOURCE: NIST SP 800-28)

Data exchanged between an HTTP server and a browser (a client of the server) to store state information on the client side and retrieve it later for server use. (SOURCE: CNSSI-4009)

**Corrective Action Plan (CAP):**

A report required to be filed semi-annually, detailing the agency's planned and completed actions to resolve findings identified during an IRS safeguard review. (SOURCE: IRS PUB 1075)

**Countermeasures:**

Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards. (SOURCE: NIST SP 800-53; NIST SP 800-37; FIPS 200)

**Covert Testing:**

Testing performed using covert methods and without the knowledge of the organization's IT staff, but with the full knowledge and permission of upper management. (SOURCE: NIST SP 800-115)

**Credential:**

An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a Subscriber. (SOURCE: NIST SP 800-63)

Evidence attesting to one's right to credit or authority. (SOURCE: FIPS 201)

Evidence or testimonials that support a claim of identity or assertion of an attribute and usually are intended to be used more than once. (SOURCE: CNSSI-4009)

**Criminal Justice Information (CJI):**

Criminal Justice Information is the term used to refer to all of the FBI Criminal Justice Information Services provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to: biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

- Biometric Data - data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. It is used to identify individuals, it can include: fingerprints, palm prints, iris scans, and facial recognition data.
- Identity History Data - textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.
- Biographic Data - information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
- Property Data - information about vehicles and property associated with a crime when accompanied by any personally identifiable information (PII).
- Case/Incident History - information about the history of criminal incidents.

(SOURCE: FBI)

**Crisis Management Plan (CMP):**

Establishing metrics to define what scenarios constitute a crisis and should consequently trigger the necessary response mechanisms. Communication that occurs within the response phase of emergency-management scenarios. Crisis-management methods of a business or an organization are called a crisis-management plan. (SOURCE: WIKIPEDIA)

**Critical Infrastructure:**

System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. [Critical Infrastructures Protection Act of 2001, 42 U.S.C. 5195c(e)] (SOURCE: CNSSI-4009)

**Criticality:**

A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function. (SOURCE: NIST SP 800-60)

**Cross-Site Scripting (XSS):**

Vulnerability that is created from insecure coding techniques, resulting in improper input validation. Often used in conjunction with CSRF and/or SQL injection. (SOURCE: PCI DSS Glossary)

**Cryptographic Algorithm:**

A well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output. (SOURCE: NIST SP 800-21; CNSSI-4009)

**Cryptographic Hash Function:**

A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties:

1. (One-way) It is computationally infeasible to find any input which maps to any pre-specified output, and
2. (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.

(SOURCE: NIST SP 800-21)

**Cryptographic Key:**

A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. (SOURCE: NIST SP 800-63)

A binary string used as a secret parameter by a cryptographic algorithm. (SOURCE: NIST SP 800-108)

A parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm. (SOURCE: FIPS 201; FIPS 198)

A parameter used in conjunction with a cryptographic algorithm that determines

- The transformation of plaintext data into ciphertext data,
- The transformation of ciphertext data into plaintext data,
- A digital signature computed from data,
- The verification of a digital signature computed from data,
- An authentication code computed from data, or
- An exchange agreement of a shared secret.

(SOURCE: FIPS 140-2)

**Cryptographic Token:**

A token where the secret is a cryptographic key. (SOURCE: NIST SP 800-63)

A portable, user-controlled physical device (e.g., smart card or PCMCIA card) used to store cryptographic information and possibly also perform cryptographic functions. (SOURCE: CNSSI-4009)

**Cryptography:**

The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification. (SOURCE: NIST SP 800-59)

The discipline that embodies principles, means, and methods for providing information security, including confidentiality, data integrity, non-repudiation, and authenticity. (SOURCE: NIST SP 800-21)

Is categorized as either secret key or public key. Secret key cryptography is based on the use of a single cryptographic key shared between two parties. The same key is used to encrypt and decrypt data. This key is kept secret by the two parties. Public key cryptography is a form of cryptography that makes use of two keys: a public key and a private key. The two keys are related but have the property that, given the public key, it is computationally infeasible to derive the private key [FIPS 140-1]. In a public key cryptosystem, each party has its own public/private key pair. The public key can be known by anyone; the private key is kept secret. (SOURCE: FIPS 191)

Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form. (SOURCE: CNSSI-4009)

**Cryptology:**

The science that deals with hidden, disguised, or encrypted communications. It includes communications security and communications intelligence. (SOURCE: NIST SP 800-60)

The mathematical science that deals with cryptanalysis and cryptography. (SOURCE: CNSSI-4009)

**Cyber Attack:**

An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. (SOURCE: CNSSI-4009)

**Cyber Incident:**

Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. See Incident. (SOURCE: CNSSI-4009)

**Cyber Infrastructure:**

Includes electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. For

example: computer systems; control systems (e.g., supervisory control and data acquisition–SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure.

(SOURCE: NISTIR 7628)

**Cybersecurity:**

The ability to protect or defend the use of cyberspace from cyberattacks. (SOURCE: CNSSI-4009)

The process of protecting information by preventing, detecting, and responding to attacks.

(SOURCE: NIST CYBERSECURITY FRAMEWORK)

**Cybersecurity Event:**

A change that may have an impact on organizational operations (including mission, capabilities, or reputation). (SOURCE: NIST CYBERSECURITY FRAMEWORK)

**Cyberspace:**

A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (SOURCE: CNSSI-4009)

**Cyclical Redundancy Check (CRC):**

A method to ensure data has not been altered after being sent through a communication channel. (SOURCE: NIST SP 800-72)

Error checking mechanism that verifies data integrity by computing a polynomial algorithm based checksum. (SOURCE: CNSSI-4009)

**Data:**

A subset of information in an electronic format that allows it to be retrieved or transmitted.

(SOURCE: CNSSI-4009)

**Data Asset:**

1. Any entity that is comprised of data. For example, a database is a data asset that is comprised of data records. A data asset may be a system or application output file, database, document, or Web page. A data asset also includes a service that may be provided to access data from an application. For example, a service that returns individual records from a database would be a data asset. Similarly, a Web site that returns data in response to specific queries (e.g., [www.weather.com](http://www.weather.com)) would be a data asset.
2. An information-based resource.

(SOURCE: CNSSI-4009)

**Data Custodian:**

Anyone with physical or operational control of a data repository, including, without limitation, roles such as database administrators, system or server administrators, backup operators and storage server administrators. (SOURCE: Data Governance Institute)

**Data Encryption Standard (DES):**

The DEA cryptographic engine that is used by the Triple Data Encryption Algorithm (TDEA). (SOURCE: NIST SP 800-67)

**Data Governance:**

The exercise of authority, control and shared decision-making (planning, monitoring and enforcement) over the management of data assets. (SOURCE: DAMA DMBOK)

A system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models, which describe who can take what actions with what information, and when, under what circumstances, using what methods. (SOURCE: Data Governance Institute)

**Data Integrity:**

The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner. (SOURCE: CNSSI-4009)

**Data Loss:**

The exposure of proprietary, sensitive, or classified information through either data theft or data leakage. (SOURCE: NIST SP 800-137)

**Data Loss Prevention (DLP):**

A system that restricts the transmission of sensitive data, reducing the risk of suffering a breach. (SOURCE: VERIZON PCI SECURITY)

**Data Privacy:**

The assurance that a person's or organization's personal and private information is not inappropriately disclosed. Ensuring Data Privacy requires Access Management, eSecurity, and other data protection efforts. (SOURCE: Data Governance Institute)

**Data Security:**

Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure. (SOURCE: CNSSI-4009)

**Decertification:**

Revocation of the certification of an information system item or equipment for cause. (SOURCE: CNSSI-4009)

**Decipher:**

Convert enciphered text to plain text by means of a cryptographic system. (SOURCE: CNSSI-4009)

**Decode:**

Convert encoded text to plain text by means of a code. (SOURCE: CNSSI-4009)

**Decrypt:**

Generic term encompassing decode and decipher. (SOURCE: CNSSI-4009)

**Decryption:**

The process of transforming ciphertext into plaintext. (SOURCE: NIST SP 800-67)

The process of changing ciphertext into plaintext using a cryptographic algorithm and key. (SOURCE: NIST SP 800-21)

Conversion of ciphertext to plaintext through the use of a cryptographic algorithm. (SOURCE: FIPS 185)

**Dedicated Mode:**

Information systems security mode of operation wherein each user, with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts, has all of the following:

1. valid security clearance for all information within the system,
2. formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, subcompartments, and/or special access programs), and
3. valid need- to-know for all information contained within the information system. When in the dedicated security mode, a system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time. (SOURCE: CNSSI-4009)

**Default Classification:**

Classification reflecting the highest classification being processed in an information system. Default classification is included in the caution statement affixed to an object. (SOURCE: CNSSI-4009)

**Defense-in-Breadth:**

A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or sub-component life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement). (SOURCE: CNSSI-4009)

**Defense-in-Depth:**

Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization.

(SOURCE: CNSSI-4009; NIST SP 800-53)

**Degauss:**

Procedure that reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Also called demagnetizing. (SOURCE: CNSSI-4009)

**Deleted File:**

A file that has been logically, but not necessarily physically, erased from the operating system, perhaps to eliminate potentially incriminating evidence. Deleting files does not always necessarily eliminate the possibility of recovering all or part of the original data. (SOURCE: NIST SP 800-72)

**Demilitarized Zone (DMZ):**

An interface on a routing firewall that is similar to the interfaces found on the firewall's protected side. Traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied. (SOURCE: NIST SP 800-41)

A host or network segment inserted as a "neutral zone" between an organization's private network and the Internet. (SOURCE: NIST SP 800-45)

Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance policy for external information exchange and to provide external, untrusted (SOURCES with restricted access to releasable information while shielding the internal networks from outside attacks. (SOURCE: CNSSI-4009)

**Denial of Service (DoS):**

The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)

(SOURCE: CNSSI-4009)

**Deny by Default / Allow by Exception:**

A firewall configuration policy that forces the user to register at the site, authenticate and authorize prior to gaining access. (SOURCE: SECUROSIS WEBSITE)

**Depth:**

An attribute associated with an assessment method that addresses the rigor and level of detail associated with the application of the method. The values for the depth attribute, hierarchically from less depth to more depth, are basic, focused, and comprehensive. (SOURCE: NIST SP 800-53A)

**Digital Evidence:**

Electronic information stored or transferred in digital form. (SOURCE: NIST SP 800-72)

**Digital Forensics:**

The application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data. (SOURCE: NIST SP 800-86)

**Digital Signature:**

An asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation. (SOURCE: NIST SP 800-63)

A non-forgeable transformation of data that allows the proof of the (SOURCE (with non-repudiation) and the verification of the integrity of that data. (SOURCE: FIPS 196)

The result of a cryptographic transformation of data which, when properly implemented, provides the services of:

1. origin authentication,
2. data integrity, and
3. signer non-repudiation.

(SOURCE: FIPS 140-2)

The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity, and signatory non-repudiation. (SOURCE: FIPS 186-3)

The result of a cryptographic transformation of data that, when properly implemented, provides origin authentication, data integrity, and signatory non-repudiation. (SOURCE: NIST SP 800-89)  
Cryptographic process used to assure data object originator authenticity, data integrity, and time stamping for prevention of replay. (SOURCE: CNSSI-4009)

**Digital Signing:**

An attempt to mimic the offline act of a person applying their signature to a paper document. Involves applying a mathematical algorithm, usually stored on and as part of the users' private key, to the contents of a body of text. This results in an encrypted version of the document (this is referred to as the 'digitally signed' document) that can only be decrypted by applying the user's public key. (Also digitally signing, digital signature)

**Direct-Attached Storage (DAS):**

A digital storage system directly attached to a server or workstation, without a storage network in between. (SOURCE: WIKIPEDIA)

**Disaster Recovery Plan (DRP):**

A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities. (SOURCE: NIST SP 800-34)

Management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. The DRP is the second plan needed by the enterprise risk managers and is used when the enterprise must recover (at its original facilities) from a loss of capability over a period of hours or days.

See Continuity of Operations Plan and Contingency Plan. (SOURCE: CNSSI-4009)

**Discretionary Access Control:**

The basis of this kind of security is that an individual user, or program operating on the user's behalf, is allowed to specify explicitly the types of access other users (or programs executing on their behalf) may have to information under the user's control. (SOURCE: FIPS 191)

A means of restricting access to objects (e.g., files, data entities) based on the identity and need-to-know of subjects (e.g., users, processes) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control). (SOURCE: CNSSI-4009)

**Disruption:**

An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction). (SOURCE: CNSSI-4009)

An unplanned event that causes an information system to be inoperable for a length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction). (SOURCE: NIST SP 800-34)

**Distributed Denial of Service – (DDoS):**

A Denial-of-Service technique that uses numerous hosts to perform the attack. (SOURCE: CNSSI-4009)

**Domain:**

A set of subjects, their information objects, and a common security policy. (SOURCE: NIST SP 800-27)

An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. See Security Domain. (SOURCE: CNSSI-4009; NIST SP 800-53; NIST SP 800-37)

**Domain Name System (DNS):**

A hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols. By providing a worldwide, distributed directory service, the Domain Name System is an essential component of the functionality on the Internet, that has been in use since 1985. (SOURCE: Wikipedia)

**Dynamic Host Configuration Protocol (DHCP):**

A standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually. (SOURCE: WIKIPEDIA)

**Eavesdropping Attack:**

An attack in which an Attacker listens passively to the authentication protocol to capture information that can be used in a subsequent active attack to masquerade as the Claimant. (SOURCE: NIST SP 800-63)

**Egress Filtering:**

Filtering of outgoing network traffic. (SOURCE: NIST SP 800-41)

**Electronic Authentication (E-authentication):**

The process of establishing confidence in user identities electronically presented to an information system. (SOURCE: NIST SP 800-63; CNSSI-4009)

**Electronic Key Entry:**

The entry of cryptographic keys into a cryptographic module using electronic methods such as a smart card or a key-loading device. (The operator of the key may have no knowledge of the value of the key being entered.) (SOURCE: FIPS 140-2)

**Electronic Key Management System (EKMS):**

Interoperable collection of systems being developed by services and agencies of the U.S. government to automate the planning, ordering, generating, distributing, storing, filling, using, and destroying of electronic key and management of other types of COMSEC material. (SOURCE: CNSSI-4009)

**Electronic Messaging Services:**

Services providing interpersonal messaging capability; meeting specific functional, management, and technical requirements; and yielding a business-quality electronic mail service suitable for the conduct of official government business. (SOURCE: CNSSI-4009)

**Electronic Signature:**

The process of applying any mark in electronic form with the intent to sign a data object. See also Digital Signature. (SOURCE: CNSSI-4009)

**Embedded Cryptographic System:**

Cryptosystem performing or controlling a function as an integral element of a larger system or subsystem. (SOURCE: CNSSI-4009)

**Embedded Cryptography:**

Cryptography engineered into an equipment or system whose basic function is not cryptographic. (SOURCE: CNSSI-4009)

**Embedded System:**

An embedded system is a computer system with a dedicated function within a larger mechanical or electrical system, often with real-time computing constraints. It is embedded as part of a complete device often including hardware and mechanical parts. Some examples of embedded systems include ATMs, cell phones, printers, thermostats, calculators, and videogame consoles. (SOURCE: Wikipedia)

**Embedded Technology:**

Specialized hardware and software that is wholly incorporated as part of a larger system or machine. (SOURCE: Army Knowledge Management and Information Technology)

**Encode:**

Convert plain text to cipher text by means of a code. (SOURCE: CNSSI-4009)

**Encrypt:**

Generic term encompassing encipher and encode. (SOURCE: CNSSI-4009)

**Encrypted Key:**

A cryptographic key that has been encrypted using an approved security function with a key encrypting key, a PIN, or a password in order to disguise the value of the underlying plaintext key. (SOURCE: FIPS 140-2)

**Encrypted Network:**

A network on which messages are encrypted (e.g., using DES, AES, or other appropriate algorithms) to prevent reading by unauthorized parties. (SOURCE: NIST SP 800-32)

**Encryption:**

Conversion of plaintext to ciphertext through the use of a cryptographic algorithm. (SOURCE: FIPS 185)

The process of changing plaintext into ciphertext for the purpose of security or privacy. (SOURCE: NIST SP 800-21; CNSSI-4009)

**Encryption Algorithm:**

Set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key. (SOURCE: CNSSI-4009)

**Encryption Certificate:**

A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes. (SOURCE: NIST SP 800-32)

**End-to-End Encryption:**

Communications encryption in which data is encrypted when being passed through a network, but routing information remains visible. (SOURCE: NIST SP 800-12)

Encryption of information at its origin and decryption at its intended destination without intermediate decryption. (SOURCE: CNSSI-4009)

**End-to-End Security:**

Safeguarding information in an information system from point of origin to point of destination. (SOURCE: CNSSI-4009)

**Endpoint:**

Any device capable of being connected, either physically or wirelessly to a network and accepts communications back and forth across the network. Endpoints include, but are not limited to, computers, servers, tablets, mobile devices, or any similar network enabled device. (SOURCE: NJCCIC)

**Enterprise:**

An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management. (SOURCE: CNSSI-4009)

**Enterprise Architecture (EA):**

The description of an enterprise's entire set of information systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture. (SOURCE: CNSSI-4009)

**Enterprise Risk Management:**

The methods and processes used by an enterprise to manage risks to its mission and to establish the trust necessary for the enterprise to support shared missions. It involves the identification of mission dependencies on enterprise capabilities, the identification and prioritization of risks

due to defined threats, the implementation of countermeasures to provide both a static risk posture and an effective dynamic response to active threats; and it assesses enterprise performance against threats and adjusts countermeasures as necessary. (SOURCE: CNSSI-40)

**Entity:**

Either a subject (an active element that operates on information or the system state) or an object (a passive element that contains or receives information). (SOURCE: NIST SP 800-27)

An active element in an open system. (SOURCE: FIPS 188)

Any participant in an authentication exchange; such a participant may be human or nonhuman, and may take the role of a claimant and/or verifier. (SOURCE: FIPS 196)

**Entrapment:**

Deliberate planting of apparent flaws in an IS for the purpose of detecting attempted penetrations. (SOURCE: CNSSI-4009)

**Entropy:**

A measure of the amount of uncertainty that an Attacker faces to determine the value of a secret. Entropy is usually stated in bits. (SOURCE: NIST SP 800-63)

**Environment:**

Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an information system. (SOURCE: FIPS 200; CNSSI-4009)

**Erasure:**

Process intended to render magnetically stored information irretrievable by normal means. (SOURCE: CNSSI-4009)

**Error Detection Code:**

A code computed from data and comprised of redundant bits of information designed to detect, but not correct, unintentional changes in the data. (SOURCE: FIPS 140-2; CNSSI-4009)

**Escrow:**

Something (e.g., a document, an encryption key) that is "delivered to a third person to be given to the grantee only upon the fulfillment of a condition." (SOURCE: FIPS 185)

**Event:**

Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring. (SOURCE: CNSSI-4009; NIST SP 800-61)

**Examination:**

A technical review that makes the evidence visible and suitable for analysis; tests performed on the evidence to determine the presence or absence of specific data. (SOURCE: NIST SP 800-72)

**Examine:**

A type of assessment method that is characterized by the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness over time. (SOURCE: NIST SP 800-53A)

**Exculpatory Evidence:**

Evidence that tends to decrease the likelihood of fault or guilt. (SOURCE: NIST SP 800-72)

**Expected Output:**

Any data collected from monitoring and assessments as part of the Information Security Continuous Monitoring (ISCM) strategy. (SOURCE: NIST SP 800-137)

**Exploit Code:**

A program that allows attackers to automatically break into a system. (SOURCE: NIST SP 800-40)

**External Information System (or Component):**

An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. (SOURCE: NIST SP 800-37; NIST SP 800-53; CNSSI-40)

**External Information System Service Provider:**

A provider of external information system services to an organization through a variety of consumer-producer relationships, including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges. (SOURCE: NIST SP 800-37; NIST SP 800-53)

**External Network:**

A network not controlled by the organization. (SOURCE: NIST SP 800-53; CNSSI-4009)

**External Party:**

A person external to New Jersey State Government.

**External Security Testing:**

Security testing conducted from outside the organization's security perimeter. (SOURCE: NIST SP 800-115)

**Extranet:**

A private network that uses Web technology, permitting the sharing of portions of an enterprise's information or operations with suppliers, vendors, partners, customers, or other enterprises. (SOURCE: CNSSI-4009)

**Failover:**

The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system. (SOURCE: NIST SP 800-53; CNSSI-4009)

**Failure Access:**

Type of incident in which unauthorized access to data results from hardware or software failure. (SOURCE: CNSSI-4009)

**Failure Control:**

Methodology used to detect imminent hardware or software failure and provide fail safe or fail soft recovery. (SOURCE: CNSSI-4009)

**False Acceptance:**

When a biometric system incorrectly identifies an individual or incorrectly verifies an impostor against a claimed identity. (SOURCE: NIST SP 800-76)

In biometrics, the instance of a security system incorrectly verifying or identifying an unauthorized person. It typically is considered the most serious of biometric security errors as it gives unauthorized users access to systems that expressly are trying to keep them out. (SOURCE: CNSSI-4009)

The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The rate given normally assumes passive impostor attempts. (SOURCE: NIST SP 800-76)

The measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's false acceptance rate typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts. (SOURCE: CNSSI-4009)

**False Positive:**

An alert that incorrectly indicates that malicious activity is occurring. (SOURCE: NIST SP 800-61)

**Federal Identity, Credentials, and Access Management (FICAM):**

The programs, processes, technologies, and personnel used to create trusted digital identity representations of individuals and NPEs, bind those identities to credentials that may serve as a proxy for the individual or NPE in access transactions, and leverage the credentials to provide authorized access to an agency's resources. ICAM cuts across numerous offices, programs, and

systems within an agency's enterprise, which are typically directed and managed separately. As a result, many of the aspects of ICAM within the Federal Government have traditionally been managed within individual stovepipes. The following figure provides a high-level overview of the complementary nature of different parts of ICAM and how concepts that were once viewed as stovepipes can intersect to provide an enterprise capability. (SOURCE: FICAM ROADMAP AND IMPLEMENTATION GUIDANCE)

**Federal Information Processing Standard (FIPS):**

A standard for adoption and use by federal departments and agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology in order to achieve a common level of quality or some level of interoperability. (SOURCE: FIPS 201)

**Federal Information Security Management Act (FISMA):**

A statute (Title III, P.L. 107-347) that requires agencies to assess risk to information systems and provide information security protections commensurate with the risk. FISMA also requires that agencies integrate information security into their capital planning and enterprise architecture processes, conduct annual information systems security reviews of all programs and systems, and report the results of those reviews to OMB. (SOURCE: CNSSI-4009)

Title III of the E-Government Act requiring each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided. (SOURCE: NIST SP 800-63)

**Federal Risk and Authorization Management Program (FedRAMP):**

A federal government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. (SOURCE: <http://cloud.cio.gov/fedramp>)

**Federal Tax Information (FTI)** – Federal Tax information consists of federal tax returns and return information (and information derived from it) that is in the agency's possession or control, which is covered by the confidentiality protections of the Internal Revenue Code (IRC) and subject to the IRC 6103(p)(4) safeguarding requirements including IRS oversight. FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to an IRC 6103(p)(2)(b) agreement. FTI includes any information created by the recipient that is derived from Federal return or return information received from the IRS or obtained through a secondary source. (SOURCE: IRS).

**File Encryption:**

The process of encrypting individual files on a storage medium and permitting access to the encrypted data only after proper authentication is provided. (SOURCE: NIST SP 800-111)

**File Protection:**

Aggregate of processes and procedures designed to inhibit unauthorized access, contamination, elimination, modification, or destruction of a file or any of its contents. (SOURCE: CNSSI-4009)

**File Security:**

Means by which access to computer files is limited to authorized users only. (SOURCE: CNSSI-4009)

**File Transfer Protocol (FTP):**

Network protocol used to transfer data from one computer to another through a public network such as the Internet. FTP is widely viewed as an insecure protocol because passwords and file contents are sent unprotected and in clear text. FTP can be implemented securely via SSH or other technology. (SOURCE: PCI DSS GLOSSARY)

**Firewall:**

A gateway that limits access between networks in accordance with local security policy. (SOURCE: NIST SP 800-32)

A hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy. (SOURCE: CNSSI-4009)

A device or program that controls the flow of network traffic between networks or hosts that employ differing security postures. (SOURCE: NIST SP 800-41)

**Firewall Control Proxy:**

The component that controls a firewall's handling of a call. The firewall control proxy can instruct the firewall to open specific ports that are needed by a call, and direct the firewall to close these ports at call termination. (SOURCE: NIST SP 800-58)

**Firmware:**

The programs and data components of a cryptographic module that are stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution. (SOURCE: FIPS 140-2)

Computer programs and data stored in hardware - typically in read- only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs. (SOURCE: CNSSI-4009)

**Flash:**

A multimedia and software platform used for creating vector graphics, animation, games and rich Internet applications (RIAs) that can be viewed, played and executed in Adobe Flash Player. Flash is frequently used to add streamed video or audio players, advertisement and interactive multimedia content to web pages. (SOURCE: WIKIPEDIA)

**Flaw:**

Error of commission, omission, or oversight in an information system that may allow protection mechanisms to be bypassed. (SOURCE: CNSSI-4009)

**Flooding:**

An attack that attempts to cause a failure in a system by providing more input than the system can process properly. (SOURCE: CNSSI-4009)

**Forensics:**

The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data. (SOURCE: CNSSI-4009)

**Frame Relay:**

A standardized wide area network (WAN) technology that specifies the physical and logical link layers of digital telecommunications channels using a packet switching methodology. Originally designed for transport across Integrated Services Digital Network (ISDN) infrastructure, it may be used today in the context of many other network interfaces. (SOURCE: WIKIPEDIA)

**Full Disk Encryption (FDE):**

The process of encrypting all the data on the hard disk drive used to boot a computer, including the computer's operating system, and permitting access to the data only after successful authentication with the full disk encryption product. (SOURCE: NIST SP 800-111)

**Function:**

A team or group of people and the tools or other resources they use to carry out one or more processes or activities. (SOURCE: ITIL V3)

**Functional Testing:**

Segment of security testing in which advertised security mechanisms of an information system are tested under operational conditions. (SOURCE: CNSSI-4009)

**Gateway:**

Interface providing compatibility between networks by converting transmission speeds, protocols, codes, or security measures. (SOURCE: CNSSI-4009)

**Gateways:**

Points (network point, device, software, etc.) that act as an entrance to another point (network, computer, software application, etc.).

**Governance:**

Ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives. (SOURCE: ISACA)

**Governance, Risk, and Compliance (GRC):**

Governance, Risk, and Compliance is a term often used by management to acknowledge the interdependencies of these three disciplines in setting policy. See also GRC-SQ and Risk Management. (SOURCE: Data Governance Institute)

**Group Authenticator:**

Used, sometimes in addition to a sign-on authenticator, to allow access to specific data or functions that may be shared by all members of a particular group. (SOURCE: CNSSI-4009)

**Hacker:**

Unauthorized user who attempts to or gains access to an information system. (SOURCE: CNSSI-4009)

**Handshaking Procedures:**

Dialogue between two information systems for synchronizing, identifying, and authenticating themselves to one another. (SOURCE: CNSSI-4009)

**Hash Value:**

The result of applying a cryptographic hash function to data (e.g., a message). (SOURCE: NIST SP 800-106)

**Hashing:**

The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data. (SOURCE: NIST SP 800-72; CNSSI-4009)

**Health information:**

means any information, whether oral or recorded in any form or medium, that:

- (a) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
- (b) relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

(SOURCE: HIPAA)

**High Availability:**

A failover feature to ensure availability during device or component interruptions.

(SOURCE: NIST SP 800-113)

**High Impact:**

The loss of confidentiality, integrity, or availability that could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States; (i.e.,

5. causes a severe degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
6. results in major damage to organizational assets;
7. results in major financial loss; or
8. results in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries).

(SOURCE: FIPS 199; CNSSI-400)

**High-Impact System:**

An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.

(SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-60; FIPS 200)

An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a potential impact value of high. (SOURCE: CNSSI-4009)

**HIPAA:**

The Health Insurance Portability and Accountability Act of 1996 (HIPAA; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996) was enacted by the United States Congress and signed by President Bill Clinton in 1996. It has been known as the Kennedy–Kassebaum Act or Kassebaum-Kennedy Act after two of its leading sponsors. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. (SOURCE: WIKIPEDIA)

**HITECH:**

The Health Information Technology for Economic and Clinical Health Act, abbreviated HITECH Act, was enacted under Title XIII of the American Recovery and Reinvestment Act of 2009 (Pub.L. 111–5). Under the HITECH Act, the United States Department of Health and Human Services is spending \$25.9 billion to promote and expand the adoption of health information technology. (SOURCE: WIKIPEDIA)

**Honeypot:**

A system (e.g., a Web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders and has no authorized users other than its administrators. (SOURCE: CNSSI-4009)

**Host:**

A computer dedicated to providing services to many users. Examples of such systems include mainframes, minicomputers, or servers that provide dynamic host configuration protocol services. (SOURCE: IRS PUB 1075)

**Hot Site:**

A fully operational offsite data processing facility equipped with hardware and software, to be used in the event of an information system disruption. (SOURCE: NIST SP 800-34)

Backup site that includes phone systems with the phone lines already connected. Networks will also be in place, with any necessary routers and switches plugged in and turned on. Desks will have desktop PCs installed and waiting, and server areas will be replete with the necessary hardware to support business-critical functions. Within a few hours, a hot site can become a fully functioning element of an organization. (SOURCE: CNSSI-4009)

**Hybrid Security Control:**

A security control that is implemented in an information system in part as a common control and in part as a system-specific control. See also Common Control and System-Specific Security Control. (SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; CNSSI-4009)

**Hypertext Transfer Protocol (HTTP):**

An application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web. Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text. HTTP is the protocol to exchange or transfer hypertext. (SOURCE: WIKIPEDIA)

**Hypertext Transfer Protocol Over Secure Socket Layer (HTTPS):**

Secure HTTP that provides authentication and encrypted communication on the World Wide Web designed for security-sensitive communication such as web-based logins. (SOURCE: PCI GLOSSARY)

**Hypervisor:**

Software or firmware responsible for hosting and managing virtual machines. For the purposes of PCI DSS, the hypervisor system component also includes the virtual machine monitor (VMM). (SOURCE: PCI DSS GLOSSARY)

**Identification:**

The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system. (SOURCE: NIST SP 800-47)

The process of discovering the true identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items. (SOURCE: FIPS 201)

An act or process that presents an identifier to a system so that the system can recognize a system entity (e.g., user, process, or device) and distinguish that entity from all others. (SOURCE: CNSSI-4009)

**Identifier:**

Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers. (SOURCE: FIPS 201)

A data object - often, a printable, non-blank character string - that definitively represents a specific identity of a system entity, distinguishing that identity from all others. (SOURCE: CNSSI-4009)

**Identity:**

A set of attributes that uniquely describe a person within a given context. (SOURCE: NIST SP 800-63)

The set of physical and behavioral characteristics by which an individual is uniquely recognizable. (SOURCE: FIPS 201)

The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity. (SOURCE: CNSSI-4009)

**Identity Proofing:**

The process by which a Credentials Service Provider (CSP) and a Registration Authority (RA) collect and verify information about a person for the purpose of issuing credentials to that person. (SOURCE: NIST SP 800-63)

The process of providing sufficient information (e.g., identity history, credentials, documents) to a Personal Identity Verification Registrar when attempting to establish an identity. (SOURCE: FIPS 201)

**Identity Registration:**

The process of making a person's identity known to the Personal Identity Verification (PIV) system, associating a unique identifier with that identity, and collecting and recording the person's relevant attributes into the system. (SOURCE: FIPS 201; CNSSI-4009)

**Identity Token:**

Smart card, metal key, or other physical object used to authenticate identity. (SOURCE: CNSSI-4009)

**Identity Validation:**

Tests enabling an information system to authenticate users or resources. (SOURCE: CNSSI-4009)

**Identity Verification:**

The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in the PIV Card of system and associated with the identity being claimed. (SOURCE: FIPS 201; NIST SP 800-79)

**Identity-Based Access Control:**

Access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user) where access authorizations to specific objects are assigned based on user identity. (SOURCE: NIST SP 800-53; CNSSI-4009)

**Identity-Based Security Policy:**

A security policy based on the identities and/or attributes of the object (system resource) being accessed and of the subject (user, group of users, process, or device) requesting access. (SOURCE: NIST SP 800-33)

**Individually Identifiable Health Information:**

Information that is a subset of health information, including demographic information collected from an individual, and:

- (a) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- (b) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
  - (i) That identifies the individual; or
  - (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

(SOURCE: HIPAA)

**Impact:**

The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. (SOURCE: NIST SP 800-60)

**Impact Level:**

The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. (SOURCE: CNSSI-4009)

High, Moderate, or Low security categories of an information system established in FIPS 199 which classify the intensity of a potential impact that may occur if the information system is jeopardized. (SOURCE: NIST SP 800-34)

**Inadvertent Disclosure:**

Type of incident involving accidental exposure of information to an individual not authorized access. (SOURCE: CNSSI-4009)

**Incident (ITIL):**

An unplanned interruption to an IT service, or a reduction in the quality of an IT service. Failure of a configuration item that has not yet impacted service is also an incident.

(SOURCE: ITIL V3 SERVICE OPERATION 7.2.2)

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. (SOURCE: NIST SP 800-61)

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. (SOURCE: FIPS 200; NIST SP 800-53)

An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. (SOURCE: CNSSI-4009)

**Incident Handling:**

The mitigation of violations of security policies and recommended practices. (SOURCE: NIST SP 800-61)

**Incident Response Plan (IRP):**

The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attacks against an organization's information system(s). (SOURCE: NIST SP 800-34)

The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of an incident against an organization's IT system(s). (SOURCE: CNSSI-4009)

**Indicator of Compromise (IOC):**

A forensic artifact or remnant of an intrusion that can be identified on a host or network.  
(SOURCE: RSA, DIVISION OF EMC)

**Industrial Control System:**

An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems (SCADA) used to control geographically dispersed assets, as well as distributed control systems (DCS) and smaller control systems using programmable logic controllers to control localized processes. (SOURCE: NIST)

**Information:**

Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.  
(SOURCE: CNSSI-4009)

**Information Asset:**

An information asset is any data, device, or other component of an information or communications system. Assets generally include hardware (e.g. servers, laptop and desktop computers, switches), software (e.g. commercial off the shelf and custom developed applications and support systems) and information. Assets may also be referred to as information resources or systems. (SOURCE: State of New Jersey Statewide Information Security Manual)

**Information Assurance (IA):**

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (SOURCE: NIST SP 800-59; CNSSI-4009)

**Information Owner:**

Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. See Information Steward.  
(SOURCE: FIPS 200; NIST SP 800-37; NIST SP 800-53; NIST SP 800-60; NIST SP 800-18; CNSSI-4009)

**Information Processing Facilities:**

The physical location housing any information processing system, service or infrastructure; this includes storage facilities for equipment not yet deployed or awaiting disposal.

**Information Resources:**

Information and related resources, such as personnel, equipment, funds, and information technology. (SOURCE: FIPS 200; FIPS 199; NIST SP 800-53; NIST SP 800-18; NIST SP 800-60; 44 U.S.C., Sec. 3502; CNSSI-4009)

**Information Security:**

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. (SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; NIST SP 800-18; NIST SP 800-60; CNSSI-4009; FIPS 200; FIPS 199; 44 U.S.C., Sec.3542)

Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

- Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
- Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
- Availability, which means ensuring timely and reliable access to and use of information.

(SOURCE: NIST SP 800-66; 44 U.S.C., Sec 3541)

**Information Security Architecture:**

An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans. (SOURCE: NIST SP 800-39)

**Information Security Classification:**

A system of designating security categories for information based on the impact to the business mission from loss of information confidentiality, integrity or availability (also classification, information classification, security classification).

**Information Security Continuous Monitoring (ISCM):**

Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

Note: The terms "continuous" and "ongoing" in this context mean that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information. (SOURCE: NIST SP 800-137)

**Information Security Policy:**

Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.

(SOURCE: NIST SP 800-53; NIST SP 800-37; NIST SP 800-18; CNSSI-4009)

**Information Security Risk:**

The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for

unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems. See Risk. (SOURCE: NIST SP 800-30)

**Information System:**

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (SOURCE: FIPS 200; FIPS 199; NIST SP 800-53A; NIST SP 800-37; NIST SP 800-60; NIST SP 800-18; 44 U.S.C., Sec. 3502; OMB Circular A-130, App. III)

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems. (SOURCE: NIST SP 800-53; CNSSI-4009)

**Information System Contingency Plan (ISCP):**

Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters. (SOURCE: NIST SP 800-34)

**Information System Owner:**

(a.k.a. Program Manager) Individual responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. (SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-18; NIST SP 800-60)

**Information System Resilience:**

The ability of an information system to continue to operate while under attack, even if in a degraded or debilitated state, and to rapidly recover operational capabilities for essential functions after a successful attack. (SOURCE: NIST SP 800-30)

The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs. (SOURCE: NIST SP 800-39)

**Information System Security Officer (ISSO):**

Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program. (SOURCE: NIST SP 800-37; NIST SP 800-53)

Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program. (SOURCE: NIST SP 800-53A; NIST SP 800-60)

**Information System-Related Security Risks:**

Information system-related security risks are those risks that arise through the loss of confidentiality, integrity, or availability of information or information systems and consider impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the Nation). See Risk. (SOURCE: NIST SP 800-37; NIST SP 800-53A)

**Information Systems Security Officer (ISSO):**

Individual assigned responsibility for maintaining the appropriate operational security posture for an information system or program. (SOURCE: CNSSI-4009)

Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program. (SOURCE: NIST SP 800-39)

**Information System Service:**

A capability provided by an information system that facilitates information processing, storage, or transmission. Also referred to as a service.

**Information Technology:**

Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which:

1. Requires the use of such equipment; or
2. Requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.

The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

(SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; NIST SP 800-18; NIST SP 800-60; FIPS 200; FIPS 199; CNSSI-4009; 40 U.S.C., Sec. 11101 and Sec 1401)

**Information Technology Resources:**

Information and communications technologies, including data, information systems, network services (e.g., Web services; messaging services); computers (e.g., hardware, software); telecommunications networks and associated assets (e.g., telephones, facsimiles, cell phones, laptops, personal digital assistants)

**Information Type:**

A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.

(SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; NIST SP 800-18; NIST SP 800-60; FIPS 200; FIPS 199; CNSSI-4009)

**Infrastructure as a Service:**

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls). (SOURCE: Cloud Security Alliance)

**Ingress Filtering:**

Method of filtering inbound network traffic such that only explicitly allowed traffic is permitted to enter the network. (SOURCE: PCI DSS GLOSSARY)

**Injection Flaws:**

Vulnerability that is created from insecure coding techniques resulting in improper input validation, which allows attackers to relay malicious code through a web application to the underlying system. This class of vulnerabilities includes SQL injection, LDAP injection, and XPath injection. (SOURCE: PCI DSS GLOSSARY)

**Insecure Protocol/Service/Port:**

A protocol, service, or port that introduces security concerns due to the lack of controls over confidentiality and/or integrity. These security concerns include services, protocols, or ports that transmit data or authentication credentials (for example, password/passphrase) in clear-text over the Internet, or that easily allow for exploitation by default or if misconfigured. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2. (SOURCE: PCI DSS GLOSSARY)

**Inside Threat:**

An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service. (SOURCE: NIST SP 800-32)

**Integrity:**

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

(SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-18; NIST SP 800-27; NIST SP 800-37; NIST SP 800-60; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542)

The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner. (SOURCE: FIPS 140-2)

The property whereby an entity has not been modified in an unauthorized manner. (SOURCE: CNSSI-4009)

**Integrity Check Value:**

Checksum capable of detecting modification of an information system. (SOURCE: CNSSI-4009)

**Intellectual Property:**

Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation. (SOURCE: NIST SP 800-32)

Creations of the mind such as musical, literary, and artistic works; inventions; and symbols, names, images, and designs used in commerce, including copyrights, trademarks, patents, and related rights. Under intellectual property law, the holder of one of these abstract “properties” has certain exclusive rights to the creative work, commercial symbol, or invention by which it is covered. (SOURCE: CNSSI-4009)

**Interconnection Security Agreement (ISA):**

An agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement (MOU/A) between the organizations. (SOURCE: NIST SP 800-47)

A document that regulates security-relevant aspects of an intended connection between an agency and an external system. It regulates the security interface between any two systems operating under two different distinct authorities. It includes a variety of descriptive, technical, procedural, and planning information. It is usually preceded by a formal MOA/MOU that defines high-level roles and responsibilities in management of a cross-domain connection. (SOURCE: CNSSI-4009)

**Interface:**

A shared boundary across which two or more separate components of a computer system exchange information. The exchange can be between software, computer hardware, peripheral devices, humans and combinations of these. (SOURCE: Wikipedia)

Common boundary between independent systems or modules where interactions take place. (SOURCE: CNSSI-4009)

**Internal Network:**

A network where:

- (a) the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or
- (b) cryptographic encapsulation or similar security technology provides the same effect.

An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned. (SOURCE: NIST SP 800-53; CNSSI-4009)

**Internal Revenue Service (IRS) Publication (Pub) 1075:**

This publication provides guidance to ensure the policies, practices, controls, and safeguards employed by recipient agencies, agents, or contractors adequately protect the confidentiality of Federal Taxpayer Information (FTI). (SOURCE: IRS PUB. 1075)

**Internal Security Controls:**

Hardware, firmware, or software features within an information system that restrict access to resources only to authorized subjects. (SOURCE: CNSSI-4009)

**Internal Security Testing:**

Security testing conducted from inside the organization's security perimeter. (SOURCE: NIST SP 800-115)

**International Organization for Standardization (ISO):**

Non-governmental organization consisting of a network of the national standards institutes. (SOURCE: PCI DSS GLOSSARY)

**Internet:**

The single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share

- a. the protocol suite specified by the Internet Architecture Board (IAB), and
- b. the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN).

(SOURCE: CNSSI-4009)

**Internet Group Management Protocol (IGMP):**

A communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships. IGMP is an integral part of IP multicast. IGMP can be used for one-to-many networking applications such as online streaming video and gaming, and allows more efficient use of resources when supporting these types of applications. (SOURCE: Wikipedia)

**Internet of Things (IoT):**

The network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and network connectivity which enables these objects to connect and exchange data. (SOURCE: Wikipedia)

**Internet Message Access Protocol (IMAP):**

An application-layer Internet protocol that allows an e-mail client to access e-mail on a remote mail server. (SOURCE: PCI DSS GLOSSARY)

**Internet Protocol (IP):**

Standard protocol for transmission of data from (SOURCE to destinations in packet-switched communications networks and interconnected systems of such networks. (SOURCE: CNSSI-4009)

**Internet Protocol Telephony (IP Telephony):**

See Voice over Internet Protocol (VoIP).

**Interoperability:**

The ability of making systems and organizations to work together (inter-operate). While the term was initially defined for information technology or systems engineering services to allow for information exchange, a more broad definition takes into account social, political, and organizational factors that impact system to system performance. (SOURCE: Wikipedia)

**Intranet:**

A private network that is employed within the confines of a given enterprise (e.g., internal to a business or agency). (SOURCE: CNSSI-4009)

**Intrusion:**

Unauthorized act of bypassing the security mechanisms of a system. (SOURCE: CNSSI-4009)

**Intrusion Detection Systems (IDS):**

Hardware or software product that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations.) (SOURCE: CNSSI-4009)

**Intrusion Prevention Systems (IPS):**

Network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it. (SOURCE: Wikipedia)

**IP Security (IPsec):**

Suite of protocols for securing Internet Protocol (IP) communications at the network layer, layer 3 of the OSI model by authenticating and/or encrypting each IP packet in a data stream. IPsec also includes protocols for cryptographic key establishment. (SOURCE: CNSSI-4009)

**ISO27000:**

A family of standards published by the International Organization for Standardization designed to keep information assets secure. ISO 27001 provides requirements for an information security management system. (SOURCE: ISO WEBSITE)

**IT Governance:**

The leadership, organizational structures, and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategies and objectives. (SOURCE: The IT Governance Institute)

**IT Infrastructure Library (ITIL):**

A public framework that describes best practice in IT service management. (SOURCE: ITIL V3)

A series of publications providing Best Practice guidance for IT Service Management. (SOURCE: Data Governance Institute)

**IT Portfolio Management:**

A key function of IT Governance, IT portfolio management is the formal process for managing IT assets such as software, hardware, middleware, an IT project, internal staff, an application or external consulting. (SOURCE: Data Governance Institute)

**IT Security Architecture:**

A description of security principles and an overall approach for complying with the principles that drive the system design; i.e., guidelines on the placement and implementation of specific security services within various distributed computing environments. (SOURCE: NIST SP 800-27)

**IT Security Awareness:**

The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. (SOURCE: NIST SP 800-50)

**IT Security Awareness and Training Program:**

Explains proper rules of behavior for the use of agency IT systems and information. The program communicates IT security policies and procedures that need to be followed. (SOURCE: NIST SP 800-50; CNSSI-4009)

**IT Security Policy:**

The "documentation of IT security decisions" in an organization.

NIST SP 800-12 categorizes IT Security Policy into three basic types:

1. Program Policy—high-level policy used to create an organization's IT security program, define its scope within the organization, assign implementation responsibilities, establish strategic direction, and assign resources for implementation.
2. Issue-Specific Policies—address specific issues of concern to the organization, such as contingency planning, the use of a particular methodology for systems risk management, and implementation of new regulations or law. These policies are likely to require more frequent revision as changes in technology and related factors take place.

3. System-Specific Policies—address individual systems, such as establishing an access control list or in training users as to what system actions are permitted. These policies may vary from system to system within the same organization. In addition, policy may refer to entirely different matters, such as the specific managerial decisions setting an organization’s electronic mail (email) policy or fax security policy.

(SOURCE: NIST SP 800-35)

**IT Security Training:**

IT Security Training strives to produce relevant and needed security skills and competencies by practitioners of functional specialties other than IT security (e.g., management, systems design and development, acquisition, auditing). The most significant difference between training and awareness is that training seeks to teach skills, which allow a person to perform a specific function, while awareness seeks to focus an individual’s attention on an issue or set of issues.

The skills acquired during training are built upon the awareness foundation, in particular, upon the security basics and literacy material. (SOURCE: NIST SP 800-50)

**IT Service Management (ITSM):**

The implementation and management of Quality IT Services that meet the needs of the Business. IT Service Management is performed by IT Service Providers through an appropriate mix of people, Process and Information Technology. (Baseline IT definition) (SOURCE: Data Governance Institute)

**IT-Related Risk:**

The net mission/business impact considering

1. The likelihood that a particular threat (SOURCE will exploit, or trigger, a particular information system vulnerability, and
2. The resulting impact if this should occur. IT-related risks arise from legal liability or mission/business loss due to, but not limited to:
  - Unauthorized (malicious, non-malicious, or accidental) disclosure, modification, or destruction of information;
  - Non-malicious errors and omissions;
  - IT disruptions due to natural or man-made disasters; or
  - Failure to exercise due care and diligence in the implementation and operation of IT.

(SOURCE: NIST SP 800-27)

**Jailbreaking:**

Modification of a smartphone or other electronic device to remove restrictions imposed by the manufacturer or operator, e.g. to allow the installation of unauthorized software.

(SOURCE: State of New Jersey Statewide Information Security Manual)

**JAVA:**

A computer programming language that is concurrent, class-based, object-oriented, and specifically designed to have as few implementation dependencies as possible. It is intended to

let application developers "write once, run anywhere" (WORA), meaning that code that runs on one platform does not need to be recompiled to run on another. Java applications are typically compiled to bytecode (class file) that can run on any Java virtual machine (JVM) regardless of computer architecture. (SOURCE: Wikipedia)

**JavaScript (JS):**

A dynamic computer programming language most commonly used as part of web browsers, whose implementations allow client-side scripts to interact with the user, control the browser, communicate asynchronously, and alter the document content that is displayed. (SOURCE: Wikipedia)

**Kerberos:**

A widely used authentication protocol developed at the Massachusetts Institute of Technology (MIT). In "classic" Kerberos, users share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to communicate with another user, Bob, authenticates to the KDC and is furnished a "ticket" by the KDC to use to authenticate with Bob. When Kerberos authentication is based on passwords, the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who capture the initial user-to- KDC exchange. Longer password length and complexity provide some mitigation to this vulnerability, although sufficiently long passwords tend to be cumbersome for users. (SOURCE: NIST SP 800-63)

A means of verifying the identities of principals on an open network. It accomplishes this without relying on the authentication, trustworthiness, or physical security of hosts while assuming all packets can be read, modified and inserted at will. It uses a trust broker model and symmetric cryptography to provide authentication and authorization of users and systems on the network. (SOURCE: NIST SP 800-95)

**Key:**

A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. (SOURCE: NIST SP 800-63)

A numerical value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. (SOURCE: CNSSI-4009)

A parameter used in conjunction with a cryptographic algorithm that determines its operation. Examples applicable to this Standard include:

1. The computation of a digital signature from data, and
2. The verification of a digital signature.

(SOURCE: FIPS 186)

**Key Exchange:**

The process of exchanging public keys in order to establish secure communications. (SOURCE: NIST SP 800-32; CNSSI-4009)

**Key Logger:**

A program designed to record which keys are pressed on a computer keyboard used to obtain passwords or encryption keys and thus bypass other security measures. (SOURCE: NIST SP 800-82)

**Key Management:**

The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization. (SOURCE: FIPS 140-2; CNSSI-4009)

**Key Management Infrastructure (KMI):**

All parts – computer hardware, firmware, software, and other equipment and its documentation; facilities that house the equipment and related functions; and companion standards, policies, procedures, and doctrine that form the system that manages and supports the ordering and delivery of cryptographic material and related information products and services to users. (SOURCE: CNSSI-4009)

**Key Pair:**

Two mathematically related keys having the properties that

1. one key can be used to encrypt a message that can only be decrypted using the other key, and
2. even knowing one key, it is computationally infeasible to discover the other key. (SOURCE: NIST SP 800-32)

A public key and its corresponding private key; a key pair is used with a public key algorithm. (SOURCE: NIST SP 800-21; CNSSI-4009)

**Known Error:**

A problem that has a documented root cause and a workaround. (SOURCE: ITIL V3)

**Laptop Computer:**

A portable computer, small enough to rest on the user's lap and having a screen that closes over the keyboard like a lid. Unlike a mobile device, a laptop computer has a computer operating system, and often more robust data storage and peripheral connection capabilities. (SOURCE: Modern Technology As Instructional Devices)

**Layer Three Switch:**

Routers that switch based on Layer 3 information, using ASICs/hardware instead of the CPU/software. Layer three switches differ from layer two switches in that they process data faster using different technology. (SOURCE: Wikipedia)

**Layer Two Switch:**

Network switch utilizing Layer 2 Tunneling Protocol (L2TP), an IETF standard that can be used as an alternative protocol to Multiprotocol Label Switching (MPLS) for encapsulation of

multiprotocol Layer 2 communications traffic over IP networks. L2TP provides a pseudo-wire service. (SOURCE: Wikipedia)

**Least Functionality:**

The principle of least functionality states that only the minimum access necessary to perform an operation should be granted to a user, a process, or a program, and that access should be granted only for the minimum amount of time necessary.

**Least Privilege:**

The security objective of granting users only those accesses they need to perform their official duties. (SOURCE: NIST SP 800-12)

The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function. (SOURCE: CNSSI-4009)

**Least Trust:**

The principal that a security architecture should be designed in a way that minimizes 1) the number of components that require trust, and 2) the extent to which each component is trusted. (SOURCE: CNSSI-4009)

**Level of Protection:**

Extent to which protective measures, techniques, and procedures must be applied to information systems and networks based on risk, threat, vulnerability, system interconnectivity considerations, and information assurance needs. Levels of protection are:

1. Basic: information systems and networks requiring implementation of standard minimum security countermeasures.
2. Medium: information systems and networks requiring layering of additional safeguards above the standard minimum security countermeasures.
3. High: information systems and networks requiring the most stringent protection and rigorous security countermeasures.

(SOURCE: CNSSI-4009)

**Lightweight Directory Access Protocol (LDAP):**

Authentication and authorization data repository utilized for querying and modifying user permissions and granting access to protected internal resources. (SOURCE: PCI DSS GLOSSARY)

**Likelihood of Occurrence:**

In Information Assurance risk analysis, a weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability. (SOURCE: CNSSI-4009)

**Link Encryption:**

Link encryption encrypts all of the data along a communications path (e.g., a satellite link, telephone circuit, or T1 line). Since link encryption also encrypts routing data, communications nodes need to decrypt the data to continue routing. (SOURCE: NIST SP 800-12)

Encryption of information between nodes of a communications system. (SOURCE: CNSSI-4009)

**List-Oriented:**

Information system protection in which each protected object has a list of all subjects authorized to access it. (SOURCE: CNSSI-4009)

**Local Access:**

Access to an organizational information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network. (SOURCE: NIST SP 800-53; CNSSI-4009)

**Local Area Network (LAN):**

A group of computers and/or other devices that share a common communications line, often in a building or group of buildings. (SOURCE: PCI DSS GLOSSARY)

**Local Authority:**

Organization responsible for generating and signing user certificates in a PKI-enabled environment. (SOURCE: CNSSI-4009)

**Logical Partition (LPAR):**

A system of subdividing, or partitioning, a computer's total resources—processors, memory and storage—into smaller units that can run with their own, distinct copy of the operating system and applications. Logical partitioning is typically used to allow the use of different operating systems and applications on a single device. The partitions may or may not be configured to communicate with each other or share some resources of the server, such as network interfaces. (SOURCE: PCI DSS GLOSSARY)

**Low Impact:**

The loss of confidentiality, integrity, or availability that could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States i.e.

5. causes a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
6. results in minor damage to organizational assets;
7. results in minor financial loss; or
8. results in minor harm to individuals.

(SOURCE: CNSSI-4009)

**Low-Impact System:**

An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.

(SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-60; FIPS 200; CNSSI-4009)

**Mainframe:**

Computers that are designed to handle very large volumes of data input and output and emphasize throughput computing. Mainframes are capable of running multiple operating systems, making it appear like it is operating as multiple computers. Many legacy systems have a mainframe design. (SOURCE: PCI DSS GLOSSARY)

**Major Application:**

A major application or system is defined as any system or application that includes one or more of the following characteristics:

- (e) Includes users in more than one agency;
- (f) Costs more than \$200,000 to develop and implement (cost includes hardware, software, and contract personnel);
- (g) Any public facing web application; and/or
- (h) Any application that stores or processes sensitive information or is deemed critical to the operations of the agency.

(SOURCE: State of New Jersey Statewide Information Security Manual)

**Malicious Applets:**

Small application programs that are automatically downloaded and executed and that perform an unauthorized function on an information system. (SOURCE: CNSSI-4009)

**Malicious Code:**

Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code. (SOURCE: NIST SP 800-53; CNSSI-4009)

**Malicious Logic:**

Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. (SOURCE: CNSSI-4009)

**Malware:**

A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. (SOURCE: NIST SP 800-83)

See Malicious Code. See also Malicious Applets and Malicious Logic.

(SOURCE: NIST SP 800-53; CNSSI-4009)

A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host. (SOURCE: NIST SP 800-61)

**Man-in-the-Middle Attack (MitM):**

An attack on the authentication protocol run in which the Attacker positions himself in between the Claimant and Verifier so that he can intercept and alter data traveling between them. (SOURCE: NIST SP 800-63)

A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association. (SOURCE: CNSSI-40090)

**Management Controls:**

The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security. (SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; FIPS 200)

Actions taken to manage the development, maintenance, and use of the system, including system-specific policies, procedures and rules of behavior, individual roles and responsibilities, individual accountability, and personnel security decisions. (SOURCE: CNSSI-4009)

**Management Security Controls:**

The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information systems security. (SOURCE: CNSSI-4009)

**Mandatory Access Control (MAC):**

A means of restricting access to system resources based on the sensitivity (as represented by a label) of the information contained in the system resource and the formal authorization (i.e., clearance) of users to access information of such sensitivity. (SOURCE: NIST SP 800-44; CNSSI-4009)

Access controls (which) are driven by the results of a comparison between the user's trust level or clearance and the sensitivity designation of the information. (SOURCE: FIPS 191)

**Masking:**

In the context of PCI DSS, it is a method of concealing a segment of data when displayed or printed. Masking is used when there is no business requirement to view the entire PAN. Masking relates to protection of PAN when displayed or printed. See Truncation for protection of PAN when stored in files, databases, etc. (SOURCE: PCI DSS GLOSSARY)

**Masquerading:**

When an unauthorized agent claims the identity of another agent, it is said to be masquerading. (SOURCE: NIST SP 800-19)

A type of threat action whereby an unauthorized entity gains access to a system or performs a malicious act by illegitimately posing as an authorized entity. (SOURCE: CNSSI-4009)

**Maximum Tolerable Downtime (MTD):**

The amount of time mission/business process can be disrupted without causing significant harm to the organization’s mission. (SOURCE: NIST SP 800-34)

**Media:**

Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, Large Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system. (SOURCE: FIPS 200; NIST SP 800-53; CNSSI-4009)

**Media Sanitization:**

A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means. (SOURCE: NIST SP 800-88)

The actions taken to render data written on media unrecoverable by both ordinary and extraordinary means. (SOURCE: CNSSI-4009)

**Memorandum of Understanding/Agreement (MOU/A):**

A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide, an MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection. (SOURCE: NIST SP 800-47; CNSSI-4009)

**Memory-Scraping Attacks:**

Malware activity that examines and extracts data that resides in memory as it is being processed or which has not been properly flushed or overwritten. (SOURCE: PCI DSS GLOSSARY)

**Message Authentication Code (MAC):**

A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data. MACs provide authenticity and integrity protection, but not non- repudiation protection. (SOURCE: NIST SP 800-63; FIPS 201)

A cryptographic checksum that results from passing data through a message authentication algorithm. (SOURCE: FIPS 198)

**Metadata:**

Data about data. The definition and scope of metadata depends upon context. In the context of Information Management, metadata is generally thought of as providing information (what database stores it? what data type is it? how long is the field? etc.) about a data element. Within the context of Data Governance, the term also includes “business” metadata such as the names

and roles of Data Stewards. Metadata repositories are employed to store and report on metadata. (SOURCE: Data Governance Institute)

**MIME:**

See Multipurpose Internet Mail Extensions.

**Minor Application:**

An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system. (SOURCE: NIST SP 800-18)

**Mobile Application Management (MAM):**

Mobile Application Management (MAM) and Mobile Application Store (MAS) management perform application monitoring, reporting, security, and deployment. (SOURCE: GSA.gov)

**Mobile Code:**

Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient. (SOURCE: NIST SP 800-53; NIST SP 800-18; CNSI-4009)

A program (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics. (SOURCE: NIST SP 800-28)

**Mobile Device:**

For the purposes of the Mobile Device Management Policy included in this Manual, a Mobile Device is any smartphone or tablet device that transmits, stores, and receives data, text, and/or voice with a connection to a wireless LAN and/or cellular network. (SOURCE: State of New Jersey Statewide Information Security Manual)

Other definitions of a Mobile Device include:

Portable cartridge/disk-based, removable storage media (e.g., floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory).

Portable computing and communications device with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). (SOURCE: NIST SP 800-53)

**Mobile Device Management (MDM):**

Mobile device management (MDM) is software that allows IT administrators to control, secure and enforce policies on smartphones, tablets and other endpoints. (SOURCE: whatis.com)

**Mode of Operation:**

An algorithm for the cryptographic transformation of data that features a symmetric key block cipher algorithm. (SOURCE: NIST SP 800-38C)

Description of the conditions under which an information system operates based on the sensitivity of information processed and the clearance levels, formal access approvals, and need-to-know of its users. Four modes of operation are authorized for processing or transmitting information: dedicated mode, system high mode, compartmented/partitioned mode, and multilevel mode. (SOURCE: CNSSI-4009)

**Moderate Impact:**

The loss of confidentiality, integrity, or availability that could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States i.e.

5. Causes a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
6. Results in significant damage to organizational assets;
7. Results in significant financial loss; or
8. Results in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.

(SOURCE: CNSSI-4009)

**Multi-Homed Connection:**

A host connected to two or more networks or having two or more network addresses. For example, a computer may be connected to multiple Local Area Networks (LANs).

(SOURCE: State of New Jersey Statewide Information Security Manual)

**Multi-Protocol Label Switching (MPLS):**

A standards-approved technology for speeding up network traffic flow and making it easier to manage. MPLS involves setting up a specific path for a given sequence of packets, identified by a label put in each packet, thus saving the time needed for a router to look up the address to the next node to forward the packet to. MPLS is called multi-protocol because it works with the Internet Protocol (IP), Asynchronous Transport Mode (ATM), and frame relay network protocols. In addition to moving traffic faster overall, MPLS makes it easy to manage a network for quality of service (QoS).

(SOURCE: Method and System for Detecting A Connection Fault)

**Multi-Factor Authentication:**

Authentication using two or more factors to achieve authentication. Factors include:

- a. something you know (e.g. password/PIN);
- b. something you have (e.g., cryptographic identification device, token); or
- c. something you are (e.g., biometric). See Authenticator.

(SOURCE: NIST SP 800-53)

**Multiprotocol Label Switching (MPLS):**

A mechanism in high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. The labels identify virtual links (paths) between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols. MPLS supports a range of access technologies, including T1/E1, ATM, Frame Relay, and DSL. (SOURCE: Wikipedia)

**Multipurpose Internet Mail Extensions (MIME):**

An Internet standard that extends the format of email to support:

- Text in character sets other than ASCII
- Non-text attachments
- Message bodies with multiple parts
- Header information in non-ASCII character sets

Although MIME was designed mainly for SMTP protocol, its use today has grown beyond describing the content of email and now often includes descriptions of content type in general, including for the web (see Internet media type) and as a storage for rich content in some commercial products. Virtually all human-written Internet email and a large proportion of automated email are transmitted via SMTP in MIME format. Internet email is so closely associated with the SMTP and MIME standards that it is sometimes called SMTP/MIME email. (SOURCE: Wikipedia)

**Mutual Authentication:**

Occurs when parties at both ends of a communication activity authenticate each other.

(SOURCE: NIST SP 800-32)

The process of both entities involved in a transaction verifying each other. (SOURCE: CNSSI-4009)

**National Institute of Standards and Technology:**

A measurement standards laboratory that is a non-regulatory agency of the United States Department of Commerce. The institute's official mission is to: Promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

The Information Technology Laboratory (ITL), one of several components within NIST, publishes standards concerning information security. (SOURCE: Wikipedia)

**Need-To-Know:**

A method of isolating information resources based on a user's need to have access to that resource in order to perform their job but no more. The terms 'need-to know' and "least privilege" express the same idea. Need-to-know is generally applied to people, while least privilege is generally applied to processes. (SOURCE: CNSSI-4009)

**Network:**

Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. (SOURCE: NIST SP 800-53; CNSSI-4009)

**Network Access:**

Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet). (SOURCE: NIST SP 800-53; CNSSI-4009)

**Network Access Control (NAC):**

A feature provided by some firewalls that allows access based on a user's credentials and the results of health checks performed on the telework client device. (SOURCE: NIST SP 800-41)

**Network Address Translation (NAT):**

A routing technology used by many firewalls to hide internal system addresses from an external network through use of an addressing schema. (SOURCE: NIST SP 800-41)

**Network Resilience:**

A computing infrastructure that provides continuous business operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged), rapid recovery if failure does occur, and the ability to scale to meet rapid or unpredictable demands. (SOURCE: CNSSI-4009)

**Network Security Scan:**

Process by which an entity's systems are remotely checked for vulnerabilities through use of manual or automated tools. Security scans that include probing internal and external systems and reporting on services exposed to the network. Scans may identify vulnerabilities in operating systems, services, and devices that could be used by malicious individuals. (SOURCE: PCI DSS GLOSSARY)

**Network Sniffing:**

A passive technique that monitors network communication, decodes protocols, and examines headers and payloads for information of interest. It is both a review technique and a target identification and analysis technique. (SOURCE: NIST SP 800-115)

**Network Time Protocol (NTP):**

A networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. (SOURCE: Wikipedia)

**Network Weaving:**

Penetration technique in which different communication networks are linked to access an information system to avoid detection and trace-back. (SOURCE: CNSSI-4009)

**Network-attached Storage (NAS):**

A file-level computer data storage connected to a computer network providing data access to a heterogeneous group of clients. (SOURCE: Wikipedia)

**Network-Level Connection:**

The connection provides access to a State Agency's private network through tunneling or a remote desktop access architecture and the software and data that reside on the internal information assets. (SOURCE: State of New Jersey Statewide Information Security Manual)

**Non-Console Access:**

Refers to logical access to a system component that occurs over a network interface rather than via a direct, physical connection to the system component. Non-console access includes access from within local/internal networks as well as access from external, or remote, networks. (SOURCE: Payment Card Industry Data Security Standards (PCI-DSS))

**Nonpublic Information:**

Information that the employee obtains, or is provided access to, during his/her employment with the State of New Jersey that the employee knows, or reasonably should know, has not been made available to the public. It includes information that the employee knows, or reasonably should know:

- (a) Is designated by the State or the Agency for which the Employee works as nonpublic information;
- (b) Contains markings such as "Confidential", "Internal", "Restricted", or similar language, or is considered sensitive information;
- (c) Contains information that must be protected by State or Federal Statute, State or Agency policy, or other regulation;
- (d) Is provided to the State or the Agency for which the employee works by customers or third parties under agreement and with the understanding that it will be treated as confidential, nonpublic information; or

Contains information related to the internal State or Agency capabilities and operations that is not available to the public, or that an individual could use to negotiate or otherwise circumvent security controls. (SOURCE: State of New Jersey Statewide Information Security Manual)

**Non-Repudiation:**

Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. (SOURCE: CNSI-4009; NIST SP 800-60)

Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.

(SOURCE: NIST SP 800-53; NIST SP 800-18)

It is the security service by which the entities involved in a communication cannot deny having participate. Specifically, the sending entity cannot deny having sent a message (non-repudiation with proof of origin), and the receiving entity cannot deny having received a message (non-repudiation with proof of delivery). (SOURCE: FIPS 191)

A service that is used to provide assurance of the integrity and origin of data in such a way that the integrity and origin can be verified and validated by a third party as having originated from a specific entity in possession of the private key (i.e., the signatory). (SOURCE: FIPS 186)

**Null:**

Dummy letter, letter symbol, or code group inserted into an encrypted message to delay or prevent its decryption or to complete encrypted groups for transmission or transmission security purposes. (SOURCE: CNSSI-4009)

**Object:**

A passive entity that contains or receives information. (SOURCE: NIST SP 800-27)

Passive information system-related entity (e.g., devices, files, records, tables, processes, programs, domains) containing or receiving information. Access to an object implies access to the information it contains. (SOURCE: CNSSI-4009; NIST SP 800-53)

**Off-line Attack:**

An attack where the Attacker obtains some data (typically by eavesdropping on an authentication protocol run, or by penetrating a system and stealing security files) that he/she is able to analyze in a system of his/her own choosing. (SOURCE: NIST SP 800-63)

**One-Way Hash Algorithm:**

Hash algorithms which map arbitrarily long inputs into a fixed-size output such that it is very difficult (computationally infeasible) to find two different hash inputs that produce the same output. Such algorithms are an essential part of the process of producing fixed-size digital signatures that can both authenticate the signer and provide for data integrity checking (detection of input modification after signature). (SOURCE: NIST SP 800-49; CNSSI-4009)

**Online Attack:**

An attack against an authentication protocol where the Attacker either assumes the role of a Claimant with a genuine Verifier or actively alters the authentication channel. The goal of the attack may be to gain authenticated access or learn authentication secrets. (SOURCE: NIST SP 800-63)

**Open Shortest Path First (OSPF):**

A link-state routing protocol for Internet Protocol (IP) networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS). It is defined as OSPF Version 2 in RFC 2328 (1998) for IPv4. The updates for IPv6 are specified as OSPF Version 3 in RFC 5340 (2008). (SOURCE: Wikipedia)

**Open Web Application Security Project (OWASP):**

A non-profit organization focused on improving the security of application software. OWASP maintains a list of critical vulnerabilities for web applications. (SOURCE: PCI DSS GLOSSARY)

**Operational Technology:**

The use of computers to monitor or alter the physical state of a system, such as the control system for a power station or the control network for a rail system. The term has become established to demonstrate the technological and functional differences between traditional IT systems and Industrial Control Systems environment. (SOURCE: Wikipedia)

**Organizational Information Security Continuous Monitoring:**

Ongoing monitoring sufficient to ensure and assure effectiveness of security controls related to systems, networks, and cyberspace, by assessing security control implementation and organizational security status in accordance with organizational risk tolerance – and within a reporting structure designed to make real-time, data-driven risk management decisions. (SOURCE: NIST SP 800-137)

**Outside Threat:**

An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service. (SOURCE: NIST SP 800-32)

**Overwrite Procedure:**

A software process that replaces data previously stored on storage media with a predetermined set of meaningless data or random patterns. (SOURCE: CNSSI-4009)

**Packet Filter:**

A routing device that provides access control functionality for host addresses and communication sessions. (SOURCE: NIST SP 800-41)

**Packet Sniffer:**

Software that observes and records network traffic. (SOURCE: CNSSI-4009)

**Parity:**

Bit(s) used to determine whether a block of data has been altered. (SOURCE: CNSSI-4009)

**Partitioning:**

A file format in which the file is divided into multiple sub files and a directory is established to locate each sub file. (SOURCE: ISACA)

**Passive Attack:**

An attack against an authentication protocol where the Attacker intercepts data traveling along the network between the Claimant and Verifier, but does not alter the data (i.e., eavesdropping).

(SOURCE: NIST SP 800-63)

An attack that does not alter systems or data. (SOURCE: CNSSI-4009)

**Passive Security Testing:**

Security testing that does not involve any direct interaction with the targets, such as sending packets to a target. (SOURCE: NIST SP 800-115)

**Password:**

A secret that a Claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings. (SOURCE: NIST SP 800-63)

A protected character string used to authenticate the identity of a computer system user or to authorize access to system resources. (SOURCE: FIPS 181)

A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization. (SOURCE: FIPS 140-2)

A protected/private string of letters, numbers, and/or special characters used to authenticate an identity or to authorize access to data. (SOURCE: CNSSI-4009)

**Password Cracking:**

The process of recovering secret passwords stored in a computer system or transmitted over a network. (SOURCE: NIST SP 800-115)

**Password Protected:**

The ability to protect a file using a password access control, protecting the data contents from being viewed with the appropriate viewer unless the proper password is entered. (SOURCE: NIST SP 800-72)

The ability to protect the contents of a file or device from being accessed until the correct password is entered. (SOURCE: NIST SP 800-124)

**Patch:**

An update to an operating system, application, or other software issued specifically to correct particular problems with the software. (SOURCE: NIST SP 800-123)

**Patch Management:**

The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs. (SOURCE: CNSSI-4009)

**Payment Card Industry (PCI):**

The term refers to the Payment Card Industry Security Standards Council, a council originally formed by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International.

The PCI Council formed a body of security standards known as the PCI Data Security Standards, (PCI DSS), and these standards consist of 12 significant requirements including multiple sub-requirements that contain numerous directives against which businesses may measure their own payment card security policies, procedures and guidelines. By complying with qualified assessments of these standards, businesses can become accepted by the PCI Standards Council as compliant with the 12 requirements, and thus receive a compliance certification and a listing on the PCI Standards Council website. Compliance efforts and acceptance must be completed on a periodic basis.

(SOURCE: Wikipedia)

**Payment Card Industry Data Security Standard (PCI DSS):**

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.

Defined by the Payment Card Industry Security Standards Council, the standard was created to increase controls around cardholder data to reduce credit card fraud via its exposure. Validation of compliance is performed annually, either by an external Qualified Security Assessor (QSA) that creates a Report on Compliance (ROC) for organizations handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes. (SOURCE: Wikipedia)

**Private Branch Exchange (PBX):**

A telephone system within an enterprise that switches calls between enterprise users on local lines while allowing all users to share a certain number of external phone lines. The main purpose of a PBX is to save the cost of requiring a line for each user to the telephone company's central office.

**Penetration Testing:**

A test methodology in which assessors, using all available documentation (e.g., system design, (SOURCE code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system. (SOURCE: NIST SP 800-53A; NIST SP 800-53; CNSSI-4009)

Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on

a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability. (SOURCE: NIST SP 800-115)

**Perishable Data:**

Information whose value can decrease substantially during a specified time. A significant decrease in value occurs when the operational circumstances change to the extent that the information is no longer useful. (SOURCE: CNSSI-4009)

**Personal Firewall:**

A utility on a computer that monitors network activity and blocks communications that are unauthorized. (SOURCE: NIST SP 800-69)

**Personal Identification Number (PIN):**

A password consisting only of decimal digits. (SOURCE: NIST SP 800-63)

A secret that a claimant memorizes and uses to authenticate his or her identity. PINs are generally only decimal digits. (SOURCE: FIPS 201)

An alphanumeric code or password used to authenticate an identity. (SOURCE: FIPS 140-2)

A short numeric code used to confirm identity. (SOURCE: CNSSI-4009)

**Personal Information (PI):**

An individual's first name or first initial and last name linked with any one or more of the following data elements:

1. Social Security number;
2. Driver's license number or State identification card number; or
3. Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data. [N.J.S.A. 2C:56:8-161]

“Personal Information” as defined by N.J.S.A. 39:2-3.3 “Personal Information” means information that identifies an individual, including an individual’s photograph; social security number; driver identification number; name; address other than the five-digit zip code; telephone number; and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver’s status. [N.J.S.A. 39:2-3.3]

**Personally Identifiable Information (PII):**

Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc. (SOURCE: CNSSI-4009)

Any information about an individual maintained by an agency, including

- a. any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and
- b. any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

(SOURCE: NIST SP 800-122)

**Phishing:**

Tricking individuals into disclosing sensitive personal information through deceptive computer-based means. (SOURCE: NIST SP 800-83)

Deceiving individuals into disclosing sensitive personal information through deceptive computer-based means. (SOURCE: CNSSI-4009)

A digital form of social engineering that uses authentic-looking—but bogus—emails to request information from users or direct them to a fake Web site that requests information.

(SOURCE: NIST SP 800-115)

**PII Confidentiality Impact Level:**

The PII confidentiality impact level—low, moderate, or high— indicates the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. (SOURCE: NIST SP 800-122)

**Plaintext:**

Data input to the Cipher or output from the Inverse Cipher. (SOURCE: FIPS 197)

Intelligible data that has meaning and can be understood without the application of decryption. (SOURCE: NIST SP 800-21)

Unencrypted information. (SOURCE: CNSSI-4009)

**Platform as a Service:**

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. (SOURCE: Cloud Security Alliance)

**Policy-Based Access Control (PBAC):**

A form of access control that uses an authorization policy that is flexible in the types of evaluated parameters (e.g., identity, role, clearance, operational need, risk, and heuristics). (SOURCE: CNSSI-4009)

**Port Scanning:**

Using a program to remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports). (SOURCE: CNSSI-4009)

**Portable Storage Device:**

An information system component that can be inserted into and removed from an information system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain non-volatile memory). (SOURCE: NIST)

**Portability:**

Usability of the same software in different IT environments. The pre-requirement for portability is the generalized abstraction between the application logic and system interfaces. When software with the same functionality is produced for several computing platforms, portability is the key issue for development cost reduction. (SOURCE: Wikipedia)

**Portable Document Format (PDF):**

A file format used to present documents in a manner independent of application software, hardware, and operating systems. (SOURCE: Wikipedia)

**Portal:**

A high-level remote access architecture that is based on a server that offers teleworkers access to one or more applications through a single centralized interface. (SOURCE: NIST SP 800-46)

**Post Office Protocol v3 (POP3):**

Application-layer protocol used by e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection. (SOURCE: PCI DSS GLOSSARY)

**Potential Impact:**

The loss of confidentiality, integrity, or availability could be expected to have:

1. A limited adverse effect (FIPS 199 low);
2. A serious adverse effect (FIPS 199 moderate); or
3. A severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.

(SOURCE: NIST SP 800-53; NIST SP 800-60; NIST SP 800-37; FIPS 199)

The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect; a serious adverse effect, or a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. (SOURCE: FIPS 200; CNSSI-4009)

**Precursor:**

A sign that an attacker may be preparing to cause an incident. (SOURCE: NIST SP 800-61; CNSSI-4009)

**Predisposing Condition:**

A condition that exists within an organization, a mission/business process, enterprise architecture, or information system including its environment of operation, which contributes to (i.e., increases or decreases) the likelihood that one or more threat events, once initiated, will result in undesirable consequences or adverse impact to organizational operations and assets, individuals, other organizations, or the Nation. (SOURCE: NIST SP 800-30)

**Print Suppression:**

Eliminating the display of characters in order to preserve their secrecy. (SOURCE: CNSSI-4009)

**Privacy:**

Restricting access to subscriber or Relying Party information in accordance with federal law and agency policy. (SOURCE: NIST SP 800-32)

Freedom from unauthorized intrusion or disclosure of information about an individual (SOURCE: ISACA)

**Privacy Impact Assessment (PIA):**

An analysis of how information is handled:

1. to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;
2. to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and
3. to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

(SOURCE: NIST SP 800-53; NIST SP 800-18; NIST SP 800-122; CNSSI-4009; OMB Memorandum 03-22)

**Private Key:**

The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data. (SOURCE: NIST SP 800-63)

A cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public. In an asymmetric (public) cryptosystem, the private key is associated with a public key. Depending on the algorithm, the private key may be used, for example, to:

1. Compute the corresponding public key,
2. Compute a digital signature that may be verified by the corresponding public key,
3. Decrypt keys that were encrypted by the corresponding public key, or
4. Compute a shared secret during a key-agreement transaction.

(SOURCE: NIST SP 800-57 Part 1; FIPS 196; FIPS 140-2)

In an asymmetric cryptography scheme, the private or secret key of a key pair which must be kept confidential and is used to decrypt messages encrypted with the public key or to digitally sign messages, which can then be validated with the public key. (SOURCE: CNSSI-4009)

**Private Network:**

Network established by an organization that uses private IP address space. Private networks are commonly designed as local area networks. Private network access from public networks should be properly protected with the use of firewalls and routers. (SOURCE: PCI DSS GLOSSARY)

**Privilege:**

A right granted to an individual, a program, or a process. (SOURCE: CNSSI-4009)

**Privileged Account:**

An information system account with approved authorizations of a privileged user. (SOURCE: CNSSI-4009; NIST SP 800-53)

**Privileged User:**

A user that is authorized (and, therefore, trusted) to perform security- relevant functions that ordinary users are not authorized to perform. (SOURCE: NIST SP 800-53; CNSSI-4009)

**Probe:**

A technique that attempts to access a system to learn something about the system. (SOURCE: CNSSI-4009)

**Problem:**

A cause of one or more incidents. (SOURCE: ITIL V3)

**Process:**

A structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs. (SOURCE: ITIL V3)

Include formal and informal mechanisms (large and small, simple and complex) to accomplish objectives. Processes identify, measure, manage, and control risks to confidentiality, integrity, availability, privacy, and safety, and they also ensure accountability. (SOURCE: ISACA Business Model for Information Security)

**Process Manager:**

An individual accountable for operational management of a process. There may be several process managers for one process and the process manager role is often assigned to the same person carrying out the process owner role. (SOURCE: ITIL V3)

**Programmable Logic Controller (PLC) or Programmable Controller:**

An industrial digital computer which has been ruggedized and adapted for the control of manufacturing processes, such as assembly lines, or robotic devices, or any activity that requires high reliability control and ease of programming and process fault diagnosis. (SOURCE: Wikipedia)

**Promiscuous Mode:**

A configuration setting for a network interface card that causes it to accept all incoming packets that it sees, regardless of their intended destinations. (SOURCE: NIST SP 800-94)

**Protected Health Information:**

The term Protected Health Information, is composed from two definitions in Section 1171 of Part C of Subtitle F of Public Law 104-191 (August 21, 1996): Health Insurance Portability and Accountability Act of 1996: Administrative Simplification. These statutory definitions are of health information and individually identifiable health information.

**Health information** means any information, whether oral or recorded in any form or medium, that:

- (a) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
- (b) relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

**Individually Identifiable Health Information** is information that is a subset of health information, including demographic information collected from an individual, and:

- (a) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- (b) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
  - (i) That identifies the individual; or
  - (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Protected Health Information means individually identifiable health information [defined above]:

- (a) Except as provided in paragraph (b) of this definition, that is:
  - (i) Transmitted by electronic media;
  - (ii) Maintained in electronic media; or
  - (iii) Transmitted or maintained in any other form or medium.
- (b) Protected health information excludes individually identifiable health information in:
  - (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
  - (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
  - (iii) Employment records held by a covered entity in its role as employer.

The HIPAA Privacy Rule covers protected health information in any medium while the HIPAA Security Rule covers electronic protected health information.

With those definitions in place, the question becomes: what elements comprise protected health information such that if they were removed, items (i) and (ii) of (b) in the definition of individually identifiable health information would not obtain. The answer is in the de-identification standard and its two implementation specifications of the HIPAA Privacy Rule [45 CFR 164.514]:

(a) Standard: de-identification of protected health information. Health information [defined above] that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

(b) Implementation specifications: requirements for de-identification of protected health information. A covered entity may determine that health information is not individually identifiable health information only if:

- 1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:
  - (i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is subject of the information; and
  - (ii) Documents the methods and results of the analysis that justify such determination; or
- 2)
  - (i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:
    - a. Names;

- b. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
    - (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
    - (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
  - c. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date,, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
  - d. Telephone numbers;
  - e. Fax numbers;
  - f. Electronic mail addresses;
  - g. Social security numbers;
  - h. Medical record numbers;
  - i. Health plan beneficiary numbers;
  - j. Account numbers;
  - k. Certificate/license numbers;
  - l. Vehicle identifiers and serial numbers, including license plate numbers;
  - m. Device identifiers and serial numbers;
  - n. Web Universal Resource Locators (URLs);
  - o. Internet Protocol (IP) address numbers;
  - p. Biometric identifiers, including finger and voice prints;
  - q. Full face photographic images and any comparable images; and
  - r. Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and
- (ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.
  - (iii) Implementation specifications: re-identification. A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that:

- a. Derivation. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and
- b. Security. The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

(SOURCE: HIPAA)

**Protocol:**

Set of rules and formats, semantic and syntactic, permitting information systems to exchange information. (SOURCE: CNSSI-4009)

**Proxy:**

A proxy is an application that “breaks” the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it. This effectively closes the straight path between the internal and external networks making it more difficult for an attacker to obtain internal addresses and other details of the organization’s internal network. Proxy servers are available for common Internet services; for example, a Hyper Text Transfer Protocol (HTTP) proxy used for Web access, and a Simple Mail Transfer Protocol (SMTP) proxy used for email.

(SOURCE: NIST SP 800-44; CNSSI-4009)

**Proxy Agent:**

A software application running on a firewall or on a dedicated proxy server that is capable of filtering a protocol and routing it between the interfaces of the device. (SOURCE: CNSSI-4009)

**Proxy Server:**

A server that services the requests of its clients by forwarding those requests to other servers.

(SOURCE: CNSSI-4009)

**Public Key (Asymmetric) Cryptographic Algorithm:**

A cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that deriving the private key from the public key is computationally infeasible.

(SOURCE: FIPS 140-2)

**Public Key:**

The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data. (SOURCE: FIPS 201; NIST SP 800-63)

A cryptographic key, used with a public key cryptographic algorithm that is uniquely associated with an entity and may be made public. In an asymmetric (public) cryptosystem, the public key is

associated with a private key. The public key may be known by anyone and, depending on the algorithm, may be used, for example, to:

1. Verify a digital signature that is signed by the corresponding private key,
2. Encrypt keys that can be decrypted by the corresponding private key, or
3. Compute a shared secret during a key-agreement transaction.

(SOURCE: NIST SP 800-57 Part 1; FIPS 196; FIPS 140-2; CNSSI-4009)

**Public Key Certificate:**

A digital document issued and digitally signed by the private key of a Certificate authority that binds the name of a Subscriber to a public key. The certificate indicates that the Subscriber identified in the certificate has sole control and access to the private key. (SOURCE: NIST SP 800-63)

A set of data that unambiguously identifies an entity, contains the entity's public key, and is digitally signed by a trusted third party (certification authority). (SOURCE: FIPS 196)

A set of data that uniquely identifies an entity, contains the entity's public key, and is digitally signed by a trusted party, thereby binding the public key to the entity. (SOURCE: FIPS 140-2)

**Public Key Infrastructure (PKI):**

A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates. (SOURCE: NIST SP 800-32; NIST SP 800-63)

An architecture which is used to bind public keys to entities, enable other entities to verify public key bindings, revoke such bindings, and provide other services critical to managing public keys. (SOURCE: FIPS 196)

A Framework that is established to issue, maintain, and revoke public key certificates. (SOURCE: FIPS 186)

A support service to the PIV system that provides the cryptographic keys needed to perform digital signature-based identity verification and to protect communications and storage of sensitive verification system data within identity cards and the verification system. (SOURCE: FIPS 201)

The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates. (SOURCE: CNSSI-4009)

**Quality of Service (QoS):**

The measurable end-to-end performance properties of a network service, which can be guaranteed in advance by a Service-Level Agreement between a user and a service provider, so as to satisfy specific customer application requirements. Note: These properties may include throughput (bandwidth), transit delay (latency), error rates, priority, security, packet loss, packet jitter, etc.

(SOURCE: CNSSI-4009)

**Rainbow Table Attack:**

A method of data attack using a pre-computed table of hash strings (fixed-length message digest) to identify the original data (SOURCE, usually for cracking password or cardholder data hashes.

(SOURCE: PCI DSS GLOSSARY)

**Reciprocity:**

Mutual agreement among participating enterprises to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information.

(SOURCE: CNSSI-4009; NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; NIST SP 800-39)

**Record:**

According to the State of New Jersey Open Public Records Act, P.L. 2001, CHAPTER 404 N.J.S. 47:1A-1 et seq., a "Government record" or "record" means any paper, written or printed book, document, drawing, map, plan, photograph, microfilm, data processed or image processed document, information stored or maintained electronically or by sound-recording or in a similar device, or any copy thereof, that has been made, maintained or kept on file in the course of his or its official business by any officer, commission, agency or authority of the State or of any political subdivision thereof, including subordinate boards thereof, or that has been received in the course of his or its official business by any such officer, commission, agency, or authority of the State or of any political subdivision thereof, including subordinate boards thereof. The terms shall not include inter-agency or intra-agency advisory, consultative, or deliberative material.

According to N.J.S.A. 47:3-20, a "Record" or "records" means: pursuant to P.L. 1953, c.410, § 2 as amended by P.L. 1994, c.140, § 3 (N.J.S.A 47:3-16), any paper, written or printed book, document or drawing, map or plan, photograph, microfilm, data processed or image processed document, sound-recording or similar device, or any copy thereof which has been made or is required by law to be received for filing, indexing, or reproducing by any officer, commission, agency or authority of the State or of any political subdivision thereof, including subordinate boards thereof, or that has been received by any such officer, commission, agency or authority of the State or of any political subdivision thereof, including subordinate boards thereof, in connection with the transaction of public business and has been retained by such recipient or its successor as evidence of its activities or because of the information contained therein.

**Records:**

The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items). (SOURCE: NIST SP 800-53; NIST SP 800-53A; CNSSI-4009)

All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States government under federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the informational value of the data in them. [44 U.S.C. SEC. 3301] (SOURCE: FIPS 200)

**Records Management:**

The process for tagging information for records-keeping requirements as mandated in the Federal Records Act and the National Archival and Records Requirements. (SOURCE: CNSSI-4009)

**Recovery Point Objective (RPO):**

The point in time to which data must be recovered after an outage. (SOURCE: NIST SP 800-34)

**Recovery Procedures:**

Actions necessary to restore data files of an information system and computational capability after a system failure. (SOURCE: CNSSI-4009)

**Recovery Time Objective (RTO):**

The overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business processes. (SOURCE: SP800-34)

**Red Team:**

A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. (SOURCE: CNSSI 4009-2015)

**Remanence:**

Residual information remaining on storage media after clearing. See Magnetic Remanence and Clearing. (SOURCE: CNSSI-4009)

**Remediation:**

The act of correcting a vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings, or uninstalling a software application. (SOURCE: NIST SP 800-40)

The act of mitigating a vulnerability or a threat. (SOURCE: CNSSI-4009)

**Remediation Plan:**

A plan to perform the remediation of one or more threats or vulnerabilities facing an organization's systems. The plan typically includes options to remove threats and vulnerabilities and priorities for performing the remediation. (SOURCE: NIST SP 800-40)

**Remote Access:**

Access to an organizational information system by a user (or an information system acting on behalf of a user) communicating through an external network (e.g., the Internet). (SOURCE: NIST SP 800-53)

Access by users (or information systems) communicating external to an information system security perimeter. (SOURCE: NIST SP 800-18)

The ability for an organization's users to access its nonpublic computing resources from external locations other than the organization's facilities. (SOURCE: NIST SP 800-46)

Access to an organization's nonpublic information system by an authorized user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). (SOURCE: CNSSI-4009)

**Remote Desktop Access Architecture:**

A high-level remote access architecture that gives a user the ability to remotely control a particular computer at their agency from an external network. Remote desktop access architecture includes, but is not limited to, systems (local and remote) and software (e.g. Cisco AnyConnect, Citrix, GoToMyPC, Verisign Identity Protection (VIP)) that is used to facilitate and secure the remote session. The specific technologies utilized in a remote desktop access architecture are determined by the New Jersey Office of Information Technology. (SOURCE: State of New Jersey Statewide Information Security Manual)

**Removable Media:**

Portable electronic storage media such as magnetic, optical, and solid-state devices, which can be inserted into and removed from a computing device, and that is used to store text, video, audio, and image information. Such devices have no independent processing capabilities. Examples include hard disks, floppy disks, zip drives, compact disks (CDs), thumb drives, pen drives, and similar USB storage devices. (SOURCE: CNSSI-4009; NIST SP 800-53)

**Replay Attacks:**

An attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access. (SOURCE: CNSSI-4009)

**Report on Compliance (ROC):**

Report documenting detailed results from an entity's PCI DSS assessment. (SOURCE: PCI DSS GLOSSARY)

**Repository:**

A database containing information and data relating to certificates as specified in a CP; may also be referred to as a directory. (SOURCE: NIST SP 800-32)

**Representational State Transfer (REST):**

A software architectural style consisting of a coordinated set of architectural constraints applied to components, connectors, and data elements, within a distributed hypermedia system. REST ignores the details of component implementation and protocol syntax in order to focus on the roles of components, the constraints upon their interaction with other components, and their interpretation of significant data elements. (SOURCE: Wikipedia)

**Residual Risk:**

The remaining potential risk after all IT security measures are applied. There is a residual risk associated with each threat. (SOURCE: NIST SP 800-33)

Portion of risk remaining after security measures have been applied.

(SOURCE: CNSSI-4009; NIST SP 800-30)

**Residue:**

Data left in storage after information-processing operations are complete, but before degaussing or overwriting has taken place. (SOURCE: CNSSI-4009)

**Resilience:**

The ability to quickly adapt and recover from any known or unknown changes to the environment through holistic implementation of risk management, contingency, and continuity planning.

(SOURCE: NIST SP 800-34)

The ability to continue to:

- (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and
- (ii) recover to an effective operational posture in a time frame consistent with mission needs.

(SOURCE: NIST SP 800-137)

**Risk:**

The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. (SOURCE: FIPS 200; NIST SP 800-60)

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:

1. The adverse impacts that would arise if the circumstance or event occurs; and
2. The likelihood of occurrence.

Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and consider the adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. (SOURCE: NIST SP 800-37; NIST SP 800-53A NIST SP 800-53; CNSSI-4009)

**Risk Analysis:**

The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment. (SOURCE: NIST SP 800-27)

Examination of information to identify the risk to an information system. See Risk Assessment. (SOURCE: CNSSI-4009)

**Risk Assessment:**

The process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation, arising through the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis. (SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37)

The process of identifying, prioritizing, and estimating risks. This includes determining the extent to which adverse circumstances or events could impact an enterprise. Uses the results of threat and vulnerability assessments to identify risk to organizational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur. The product of a risk assessment is a list of estimated potential impacts and unmitigated vulnerabilities. Risk assessment is part of risk management and is conducted throughout the Risk Management Framework (RMF). (SOURCE: CNSSI-4009)

**Risk Management:**

The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes:

1. The conduct of a risk assessment;
2. The implementation of a risk mitigation strategy; and
3. Employment of techniques and procedures for the continuous monitoring of the security state of the information system.

(SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; CNSSI-4009; NIST SP 800-82; NIST SP 800-34)

The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes:

1. The conduct of a risk assessment;
2. The implementation of a risk mitigation strategy; and
3. Employment of techniques and procedures for the continuous monitoring of the security state of the information system.

(SOURCE: FIPS 200)

The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time. (SOURCE: NIST SP 800-39)

**Risk Mitigation:**

Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

(SOURCE: CNSSI-4009; NIST SP 800-30; NIST SP 800-39)

**Risk Monitoring:**

Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions. (SOURCE: NIST SP 800-30; NIST SP 800-39)

**Risk Tolerance:**

The level of risk an entity is willing to assume in order to achieve a potential desired result.

(SOURCE: NIST SP 800-32)

The defined impacts to an enterprise's information systems that an entity is willing to accept.

(SOURCE: CNSSI-4009)

**Rogue Device:**

An unauthorized node on a network. (SOURCE: NIST SP 800-115)

**Role:**

A group attribute that ties membership to function. When an entity assumes a role, the entity is given certain rights that belong to that role. When the entity leaves the role, those rights are removed. The rights given are consistent with the functionality that the entity needs to perform the expected tasks. (SOURCE: CNSSI-4009)

**Role-Based Access Control (RBAC):**

A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities. (SOURCE: NIST SP 800-95)

Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals. (SOURCE: NIST SP 800-53; CNSSI-4009)

**Root Cause Analysis:**

A principle-based, systems approach for the identification of underlying causes associated with a particular set of risks. (SOURCE: NIST SP 800-30; NIST SP 800-39)

**Router:**

Hardware or software that connects two or more networks. Functions as sorter and interpreter by looking at addresses and passing bits of information to proper destinations. Software routers are sometimes referred to as gateways. (SOURCE: PCI DSS GLOSSARY)

**Rule-Based Security Policy:**

A security policy based on global rules imposed for all subjects. These rules usually rely on a comparison of the sensitivity of the objects being accessed and the possession of corresponding attributes by the subjects requesting access. (SOURCE: NIST SP 800-33; CNSSI-4009)

**S/MIME (NIST)**

A set of specifications for securing electronic mail. Secure/ Multipurpose Internet Mail Extensions (S/MIME) is based upon the widely used MIME standard and describes a protocol for adding cryptographic security services through MIME encapsulation of digitally signed and encrypted objects. The basic security services offered by S/MIME are authentication, non-repudiation of origin, message integrity, and message privacy. Optional security services include signed receipts, security labels, secure mailing lists, and an extended method of identifying the signer's certificate(s).

(SOURCE: NIST SP 800-49)

**Safeguards:**

Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

(SOURCE: NIST SP 800-53; NIST SP 800-37; FIPS 200; CNSSI-4009)

**Safety:**

Condition of being protected from harm or other non-desirable outcomes. (SOURCE: Wikipedia)

**Sanitization:**

Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs. (SOURCE: FIPS 200)

A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means. (SOURCE: NIST SP 800-53; CNSSI-4009)

**Scalability:**

The ability of a system, network, or process to handle a growing amount of work in a capable manner or its ability to be enlarged to accommodate that growth. (SOURCE: WIKIPEDIA)

**Scanning:**

Sending packets or requests to another system to gain information to be used in a subsequent attack. (SOURCE: CNSSI-4009)

**Scoping:**

Process of identifying all system components, people, and processes to be included in an assessment. The first step of an assessment is to accurately determine the scope of the review. (SOURCE: PCI DSS GLOSSARY)

**Secret Key:**

A cryptographic key that is used with a secret-key (symmetric) cryptographic algorithm that is uniquely associated with one or more entities and is not made public. The use of the term “secret” in this context does not imply a classification level, but rather implies the need to protect the key from disclosure. (SOURCE: NIST SP 800-57)

A cryptographic key that is used with a symmetric cryptographic algorithm that is uniquely associated with one or more entities and is not made public. The use of the term “secret” in this context does not imply a classification level, but rather implies the need to protect the key from disclosure.

(SOURCE: CNSSI-4009)

A cryptographic key that must be protected from unauthorized disclosure to protect data encrypted with the key. The use of the term “secret” in this context does not imply a classification level; rather, the term implies the need to protect the key from disclosure or substitution. (SOURCE: FIPS 201)

A cryptographic key that is uniquely associated with one or more entities. The use of the term “secret” in this context does not imply a classification level, but rather implies the need to protect the key from disclosure or substitution. (SOURCE: FIPS 198)

A cryptographic key, used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public. (SOURCE: FIPS 140-2)

### **Secure Coding Guidelines:**

Philosophy and approach supporting the practice of developing computer software in a way that guards against the accidental introduction of security vulnerabilities. Defects, bugs and logic flaws are consistently the primary cause of commonly exploited software vulnerabilities. Through the analysis of thousands of reported vulnerabilities, security professionals have discovered that most vulnerabilities stem from a relatively small number of common software programming errors. By identifying the insecure coding practices that lead to these errors and educating developers on secure alternatives, organizations can take proactive steps to help significantly reduce or eliminate vulnerabilities in software before deployment. (SOURCE: Wikipedia)

### **Secure DNS (SEC DNS):**

Configuring and operating DNS servers so that the security goals of data integrity and authentication are achieved and maintained. (SOURCE: NIST SP 800-81)

### **Secure Hash Algorithm (SHA):**

A hash algorithm with the property that is computationally infeasible

1. To find a message that corresponds to a given message digest, or
2. To find two different messages that produce the same message digest.

(SOURCE: CNSI-4009)

### **Secure Hash Standard:**

This Standard specifies secure hash algorithms - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256 - for computing a condensed representation of electronic data (message). When a message of any length less than  $2^{64}$  bits (for SHA-1, SHA-224 and SHA-256) or less than  $2^{128}$  bits (for SHA-384, SHA-512, SHA-512/224 and SHA-512/256) is input to a hash algorithm, the result is an output called a message digest. The message digests range in length from 160 to 512 bits, depending on the algorithm. Secure hash algorithms are typically used with other cryptographic algorithms, such as digital signature algorithms and keyed-hash message authentication codes, or in the generation of random numbers (bits).

The hash algorithms specified in this Standard are called secure because, for a given algorithm, it is computationally infeasible 1) to find a message that corresponds to a given message digest, or

2) to find two different messages that produce the same message digest. Any change to a message will, with a very high probability, result in a different message digest. This will result in a verification failure when the secure hash algorithm is used with a digital signature algorithm or a keyed-hash message authentication algorithm. (SOURCE: FIPS 180-4)

Specification for a secure hash algorithm that can generate a condensed message representation called a message digest. (SOURCE: CNSSI-4009)

**Secure Shell (SSH):**

Protocol suite providing encryption for network services like remote login or remote file transfer. (SOURCE: PCI DSS GLOSSARY)

**Secure Socket Layer (SSL):**

A protocol used for protecting private information during transmission via the Internet.

Note: SSL works by using a public key to encrypt data that's transferred over the SSL connection. Most Web browsers support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with "https:" instead of "http:" (SOURCE: CNSSI-4009)

**Security:**

A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach. (SOURCE: CNSSI-4009)

**Security Assertion Markup Language (SAML):**

An XML-based security specification developed by the Organization for the Advancement of Structured Information Standards (OASIS) for exchanging authentication (and authorization) information between trusted entities over the Internet. (SOURCE: NIST SP 800-63)

A framework for exchanging authentication and authorization information. Security typically involves checking the credentials presented by a party for authentication and authorization. SAML standardizes the representation of these credentials in an XML format called "assertions," enhancing the interoperability between disparate applications. (SOURCE: NIST SP 800-95)

A protocol consisting of XML-based request and response message formats for exchanging security information, expressed in the form of assertions about subjects, between online business partners. (SOURCE: CNSSI-4009)

**Security Attribute:**

A security-related quality of an object. Security attributes may be represented as hierarchical levels, bits in a bit map, or numbers. Compartments, caveats, and release markings are examples of security attributes. (SOURCE: FIPS 188)

An abstraction representing the basic properties or characteristics of an entity with respect to safeguarding information; typically associated with internal data structures (e.g., records, buffers, files) within the information system which are used to enable the implementation of access control and flow control policies; reflect special dissemination, handling, or distribution instructions; or support other aspects of the information security policy. (SOURCE: NIST SP 800-53; CNSSI-4009)

**Security Content Automation (SCAP):**

A method for using specific standardized testing methods to enable automated vulnerability management, measurement, and policy compliance evaluation against a standardized set of security requirements. (SOURCE: CNSSI-4009)

**Security Control Assessment:**

The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; CNSSI-4009)

**Security Control Baseline:**

The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system. (SOURCE: NIST SP 800-53; FIPS 200)

One of the sets of minimum security controls defined for federal information systems in NIST Special Publication 800-53 and CNSS Instruction 1253. (SOURCE: NIST SP 800-53A)

**Security Control Effectiveness:**

The measure of correctness of implementation (i.e., how consistently the control implementation complies with the security plan) and how well the security plan meets organizational needs in accordance with current risk tolerance. (SOURCE: NIST SP 800-137)

**Security Controls:**

The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

(SOURCE: NIST SP 800-53; NIST SP 800-37; NIST SP 800-53A; NIST SP 800-60; FIPS 200; FIPS 199; CNSSI-4009)

**Security Controls Baseline:**

The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system. (SOURCE: CNSSI-4009)

**Security Domain:**

A set of subjects, their information objects, and a common security policy. (SOURCE: NIST SP 800-27)

A collection of entities to which applies a single security policy executed by a single authority. (SOURCE: FIPS 188)

A domain that implements a security policy and is administered by a single authority. (SOURCE: NIST SP 800-37; NIST SP 800-53; CNSSI-4009)

**Security Impact Analysis:**

The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.

(SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; CNSSI-4009)

**Security Information and Event Management (SIEM) Tool:**

Application that provides the ability to gather security data from information system components and present that data as actionable information via a single interface. (SOURCE: NIST SP 800-128)

**Security Objective:**

Confidentiality, integrity, or availability.

(SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-60; NIST SP 800-37; FIPS 200; FIPS 199)

**Security Plan:**

Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. See 'System Security Plan' or 'Information Security Program Plan.'

(SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; NIST SP 800-18)

**Security Policy:**

The statement of required protection of the information objects. (SOURCE: NIST SP 800-27)

A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data.

(SOURCE: FIPS 188; (SOURCE: NIST SP 800-37; NIST SP 800-53; CNSSI-4009)

**Security Requirements:**

Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

(SOURCE: FIPS 200; NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; CNSSI-4009)

**Security Safeguards:**

Protective measures and controls prescribed to meet the security requirements specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. (SOURCE: CNSSI-4009)

**Security Test & Evaluation (ST&E):**

Examination and analysis of the safeguards required to protect an information system, as they have been applied in an operational environment, to determine the security posture of that system. (SOURCE: CNSSI-4009)

**Security Testing:**

Process to determine that an information system protects data and maintains functionality as intended. (SOURCE: CNSSI-4009)

**Sensitive Data:**

Data that is private, personal, or proprietary and must be protected from unauthorized access. (SOURCE: Data Governance Institute)

**Sensitive Information:**

A term to describe any information which requires protection from unauthorized access or disclosure. (SOURCE: State of New Jersey Statewide Information Security Manual)

**Sensitive Personally Identifiable Information (SPII):**

Personal information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. (SOURCE: US DHS)

**Sensitivity:**

The degree to which an IT system or application requires protection (to ensure confidentiality, integrity, and availability) which is determined by an evaluation of the nature and criticality of the data processed, the relation of the system to the organization missions and the economic value of the system components.

**Separation of Duties:**

Practice of dividing steps in a function among different individuals, so as to keep a single individual from being able to subvert the process. (SOURCE: PCI DSS GLOSSARY)

**Service:**

A capability provided by an information system that facilitates information processing, storage, or transmission. Also referred to as an information system service.

**Service Management:**

A set of specialized organizational capabilities for providing value to customers in the form of services. (SOURCE: ITIL V3)

**Service Organization Control (SOC) - 1 Report:**

These reports, prepared in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization, are specifically intended to meet the needs of the managements of user entities and the user entities' auditors, as they evaluate the effect of the controls at the service organization on the user entities' financial statement assertions. These reports are important components of user entities' evaluation of their internal controls over financial reporting for purposes of comply with laws and regulations such as the Sarbanes-Oxley Act and the user entities' auditors as they plan and perform audits of the user entities' financial statements. There are two types of reports for these engagements:

- Type 1 – report on the fairness of the presentation of management's description of the service organization's system and the suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date.
- Type 2 – report on the fairness of the presentation of management's description of the service organization's system and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified period.

The use of these reports is restricted to the management of the service organization, user entities of the service organization and user auditors. (SOURCE: AICPA Website)

**Service Organization Control (SOC) - 2 Report:**

These reports are intended to meet the needs of a broad range of users that need information and assurance about the controls at a service organization that affect the security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems . Examples of stakeholders who may need these reports are, management or those charged with governance of the user entities and of the service organization, customers of the service organization, regulators, business partners, suppliers, and others who have an understanding of the service organization and its controls. Use of these reports generally is restricted to parties that have this understanding The AICPA Guide: Reports on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (currently under development) provides guidance for performing these engagements. These reports can play an important role in:

- Oversight of the organization

- Vendor management programs
- Internal corporate governance and risk management processes
- Regulatory oversight

Similar to a SOC 1 report there are two types of report: A type 2, report on management's description of a service organization's system and the suitability of the design and operating effectiveness of controls; and a type 1, report on management's description of a service organization's system and the suitability of the design of controls. Use of these reports is generally restricted.

(SOURCE: AICPA Website)

### **Service Organization Control (SOC) - 3 Report:**

These reports are designed to meet the needs of users who need assurance about the controls at a service organization that affect the security, availability, and processing integrity of the systems used by a service organization to process users' information, and the confidentiality, or privacy of that information, but do not have the need for or the knowledge necessary to make effective use of a SOC 2 Report.

These reports are prepared using the AICPA/Canadian Institute of Chartered Accountants (CICA) Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy. Because they are general use reports, SOC 3 reports can be freely distributed or posted on a website as a SysTrust for Service Organizations seal. For more information about the SysTrust for Service Organization seal program go to [www.webtrust.org](http://www.webtrust.org).

(SOURCE: AICPA Website)

### **Service Oriented Architecture (SOA):**

An architectural style and discipline that improves IT's ability to meet business demands. Service-oriented design principles advocate factoring system capabilities into loosely coupled, autonomous components (i.e., services) and making the capabilities available to other system components or external consumers. SOA is not dependent on any particular technology.

(SOURCE: The Burton Group (Gartner))

### **Service-Level Agreement (SLA):**

Defines the specific responsibilities of the service provider and sets the customer expectations.

(SOURCE: CNSSI-4009)

### **Session:**

A semi-permanent interactive information interchange, also known as a dialogue, a conversation or a meeting, between two or more communicating devices, or between a computer and user (see Login session). A session is set up or established at a certain point in time, and then torn down at some later point. An established communication session may involve more than one message in each direction. A session is typically, but not always, stateful, meaning that at least one of the communicating parts needs to save information about the session history in order to

be able to communicate, as opposed to stateless communication, where the communication consists of independent requests with responses. (SOURCE: Wikipedia)

**Session Initiation Protocol (SIP):**

A signaling communications protocol, widely used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP) networks. The protocol defines the messages that are sent between endpoints that govern establishment, termination and other essential elements of a call. SIP can be used for creating, modifying and terminating sessions consisting of one or several media streams. SIP can be used for two-party (unicast) or multiparty (multicast) sessions. Other SIP applications include video conferencing, streaming multimedia distribution, instant messaging, presence information, file transfer, fax over IP and online games. (SOURCE: Wikipedia)

**Signature:**

A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system. (SOURCE: NIST SP 800-61; CNSSI-4009)

**Signature Certificate:**

A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions. (SOURCE: NIST SP 800-32; CNSSI-4009)

**Signed Data:**

Data on which a digital signature is generated. (SOURCE: FIPS 196)

**Simple Mail Transfer Protocol (SMTP):**

An Internet standard for electronic mail (e-mail) transmission. (SOURCE: Wikipedia)

**Simple Network Management Protocol (SNMP):**

An Internet-standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks and more. It is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects. (SOURCE: Wikipedia)

**Simple Object Access Protocol (SOAP):**

A protocol specification for exchanging structured information in the implementation of web services in computer networks. It relies on XML Information Set for its message format, and usually relies on other application layer protocols, most notably Hypertext Transfer Protocol (HTTP) or Simple Mail Transfer Protocol (SMTP), for message negotiation and transmission. (SOURCE: Wikipedia)

**Single Point of Failure:**

A resource whose loss will result in the loss of service or production. (SOURCE: ISACA)

**SLA:**

Service Level Agreements - Defines the specific responsibilities of the service provider and sets the customer expectations. (SOURCE: NIST)

**Smartphone:**

A handheld mobile communication device with a mobile operating system and an integrated mobile broadband cellular network and Wi-Fi connection capability used for voice and data communications. (SOURCE: Wikipedia)

**Social Engineering:**

An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks. (SOURCE: NIST SP 800-61; CNSSI-4009)

A general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious. (SOURCE: NIST SP 800-114)

The process of attempting to trick someone into revealing information (e.g., a password). (SOURCE: NIST SP 800-115)

**Social Media:**

The interaction among people in which they create, share or exchange information and ideas in virtual communities and networks. (SOURCE: Wikipedia)

**Social Networking:**

Use of a platform/service to support collaboration among people who share interests, activities, backgrounds or real-life connections. A social network service consists of a representation of each user (often a profile), his social links, and a variety of additional services. Social networking is web-based services that allow individuals to create a public profile, to create a list of users with whom to share connection, and view and cross the connections within the system. Most social network services are web-based and provide means for users to interact over the Internet, such as e-mail and instant messaging. Social network sites are varied and they incorporate new information and communication tools such as, mobile connectivity, photo/video/sharing and blogging. Online community services are sometimes considered as a social network service, though in a broader sense, social network service usually means an individual-centered service whereas online community services are group-centered. Social networking sites allow users to share ideas, pictures, posts, activities, events, interests with people in their network. (SOURCE: Wikipedia)

**Software:**

Computer programs and associated data that may be dynamically written or modified during execution. (SOURCE: NIST)

**Software as a Service (SaaS):**

The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings. (SOURCE: Cloud Security Alliance)

**Software Development Life Cycle (SDLC):**

Acronym for “system development life cycle” or “software development lifecycle.” Phases of the development of a software or computer system that includes planning, analysis, design, testing, and implementation. (SOURCE: PCI DSS GLOSSARY)

**Spam:**

The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. (SOURCE: NIST NIST SP 800-53)

Unsolicited bulk commercial email messages. (SOURCE: NIST NIST SP 800-45)

Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. (SOURCE: CNSSI-4009)

**Special Character:**

Any non-alphanumeric character that can be rendered on a standard American-English keyboard. Use of a specific special character may be application-dependent. The list of special characters follows:

` ~ ! @ # \$ % ^ & \* ( ) \_ + | } { “ : ? > < [ ] \ ; ‘ , . / - =

(SOURCE: CNSSI-4009)

**Specification:**

An assessment object that includes document-based artifacts (e.g., policies, procedures, plans, system security requirements, functional specifications, and architectural designs) associated with an information system. (SOURCE: NIST SP 800-53A)

**Spillage:**

Security incident that results in the transfer of classified or CUI information onto an information system not accredited (i.e., authorized) for the appropriate security level. (SOURCE: CNSSI-4009)

**Split Tunneling:**

A computer networking concept that allows a VPN user to access a public network (e.g., the Internet) and a local LAN or WAN at the same time, using the same physical network connection.

This connection service is usually facilitated through a program such as a VPN client software application.

(SOURCE: Wikipedia)

**Spoofing:**

“IP spoofing” refers to sending a network packet that appears to come from a source other than its actual source. (SOURCE: NIST SP 800-48)

**Spyware:**

Software that covertly gathers user information through the user’s Internet connection without the user’s knowledge. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else.

Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.

(SOURCE: NIST SP 800-53; CNSSI-4009)

**SQL Injection:**

Form of attack on database-driven web site. A malicious individual executes unauthorized SQL commands by taking advantage of insecure code on a system connected to the Internet. SQL injection attacks are used to steal information from a database from which the data would normally not be available and/or to gain access to an organization’s host computers through the computer that is hosting the database. (SOURCE: PCI DSS GLOSSARY)

**Stakeholder:**

Anyone who has a responsibility for, an expectation from or some other interest in the enterprise.

(SOURCE: ISACA GLOSSARY)

**State:**

Intermediate Cipher result that can be pictured as a rectangular array of bytes. (SOURCE: FIPS 197)

**Stateful Inspection:**

Also called “dynamic packet filtering.” Firewall capability that provides enhanced security by keeping track of the state of network connections. Programmed to distinguish legitimate packets for various connections, only packets matching an established connection will be permitted by the firewall; all others will be rejected. (SOURCE: PCI DSS GLOSSARY)

**Stateless Protocol:**

A communications protocol that treats each request as an independent transaction that is unrelated to any previous request so that the communication consists of independent pairs of request and response. A stateless protocol does not require the server to retain session

information or status about each communications partner for the duration of multiple requests. Examples of stateless protocols include the Internet Protocol (IP) which is the foundation for the Internet, and the Hypertext Transfer Protocol (HTTP) which is the foundation of data communication for the World Wide Web. (SOURCE: Wikipedia)

**Storage Area Network (SAN):**

A dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system.

(SOURCE: Wikipedia)

**Strong Authentication:**

The requirement to use multiple factors for authentication and advanced technology, such as dynamic passwords or digital certificates, to verify an entity's identity. (SOURCE: CNSSI-4009)

**Strong Cryptography:**

Cryptography based on industry-tested and accepted algorithms, along with key lengths that provide a minimum of 112-bits of effective key strength and proper key-management practices. Cryptography is a method to protect data and includes both encryption and hashing. Examples of industry-tested and accepted standards and algorithms include: AES (128 bits and higher), TDES/TDEA (triple-length keys), RSA (2048 bits and higher), ECC (224 bits and higher), and DSA/D-H (2048/224 bits and higher). (SOURCE: PCI Payment Card Standards Council)

**Strong Password:**

A minimum of eight characters using a combination of upper and lowercase letters, numbers and special characters.

**Structured Query Language (SQL):**

Computer language used to create, modify, and retrieve data from relational database management systems. (SOURCE: PCI DSS GLOSSARY)

**Subject Matter Expert (SME):**

A person who is an authority in a particular area or topic. (SOURCE: Wikipedia)

**Subscriber:**

A party who receives a credential or token from a CSP (Credentials Service Provider) and becomes a claimant in an authentication protocol. (SOURCE: CNSSI-4009; NIST SP 800-63)

**Supervisory Control and Data Acquisition (SCADA):**

A control system architecture that uses computers, networked data communications and graphical user interfaces for high-level process supervisory management, but uses other peripheral devices such as programmable logic controllers and discrete PID controllers to interface to the process plant or machinery. (SOURCE: Wikipedia)

**Supplier:**

Organization or individual that enters into an agreement with the acquirer or integrator for the supply of a product or service. This includes all suppliers in the supply chain. Includes (i) developers or manufacturers of information systems, system components, or information system services; (ii) vendors; and (iii) product resellers. (SOURCE: NIST SP800-161)

**Supply Chain:**

A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers. (SOURCE: NIST SP 800-53; CNSSI-4009)

**Symmetric Key:**

A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code. (SOURCE: NIST SP 800-63; CNSSI-4009)

A single cryptographic key that is used with a secret (symmetric) key algorithm. (SOURCE: NIST SP 800-21 [2nd Ed])

**System:**

Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. (SOURCE: CNSSI-4009)

A system is defined as a discrete set of information technologies including computer hardware, software, databases, etc., organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (SOURCE: NIST)

**System Administrator:**

A person who manages the technical aspects of a system. (SOURCE: NIST SP 800-40)

Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures. (SOURCE: CNSSI-4009)

**System Assets:**

Any software, hardware, data, administrative, physical, communications, or personnel resource within an information system. (SOURCE: CNSSI-4009)

**System Development Life Cycle (SDLC):**

The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation. (SOURCE: NIST SP 800-34; CNSSI-4009)

**System Integrity:**

The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

(SOURCE: NIST SP 800-27)

Attribute of an information system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. (SOURCE: CNSSI-4009)

**System Level Object:**

Anything on a system component that is required for its operation, including but not limited to database tables, stored procedures, application executables and configuration files, system configuration files, static and shared libraries and DLLs, system executables, device drivers and device configuration files, and third-party components. (SOURCE: PCI DSS GLOSSARY)

**System Security Plan:**

Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

(SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; NIST SP 800-18; FIPS 200)

The formal document prepared by the information system owner (or common security controls owner for inherited controls) that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements. The plan can also contain as supporting appendices or as references, other key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan. (SOURCE: CNSSI-4009)

**System Software:**

The special software within the cryptographic boundary (e.g., operating system, compilers or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, associated programs, and data. (SOURCE: FIPS 140-2)

**Tablet:**

An open-faced handheld mobile communication and computing device with a mobile operating system, a touchscreen display, and an integrated Wi-Fi network capability. In some cases, tablets include cellular network connection capability. Tablets resemble smartphones with the major differences being that tablets are not typically used for voice communications and they are larger. (SOURCE: Tech Target)

**Tabletop Exercise:**

Test method that presents a limited simulation of a disruption, emergency or crisis scenario in a narrative format in which participants review and discuss, not perform, the policy, methods, procedures, coordination, and resource assignments associated with plan activation.

(SOURCE: ISO 22399:2007)

**Tailoring:**

The process by which a security control baseline is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls via explicit assignment and selection statements. (SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; CNSSI-4009)

**Tampering:**

An intentional event resulting in modification of a system, its intended behavior, or data.

(SOURCE: CNSSI-4009)

**Technical Non-Repudiation:**

The contribution of public key mechanisms to the provision of technical evidence supporting a non-repudiation security service. (SOURCE: NIST SP 800-32)

**Technology:**

Composed of the tools, applications, and infrastructure that make processes more efficient. Technology implemented by people following processes allows for the State to meet its information security objectives. (SOURCE: ISACA)

**Telephone Network Protocol (TELNET):**

Typically used to provide user-oriented command line login sessions to devices on a network. User credentials are transmitted in clear text. (SOURCE: PCI DSS GLOSSARY)

**Terminal Access Controller Access Control System (TACACS):**

Remote authentication protocol commonly used in networks that communicates between a remote access server and an authentication server to determine user access rights to the network. This authentication method may be used with a token, smart card, etc., to provide two-factor authentication. (SOURCE: PCI DSS GLOSSARY)

**Test:**

A type of assessment method that is characterized by the process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control effectiveness over time. (SOURCE: NIST SP 800-53A)

**Third Party:**

Any entity that an agency does business with. This may include suppliers, vendors, contract manufacturers, business partners and affiliates, brokers, distributors, resellers, and agents. Third parties can be both 'upstream' (suppliers and vendors) and 'downstream', (distributors and resellers) as well as non-contractual parties. (SOURCE: US Office of the Comptroller of the Currency)

**Threat:**

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. (SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-27; NIST SP 800-60; NIST SP 800-37; CNSSI-4009; FIPS 200)

The potential source of an adverse event. (SOURCE: NIST SP 800-61)

**Threat Assessment:**

Formal description and evaluation of threat to an information system. (SOURCE: NIST SP 800-53; NIST SP 800-18)

Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat. (SOURCE: CNSSI-4009; NIST SP 800-53A)

**Threat Event:**

An event or situation that has the potential for causing undesirable consequences or impact. (SOURCE: NIST SP 800-30)

**Threat Monitoring:**

Analysis, assessment, and review of audit trails and other information collected for the purpose of searching out system events that may constitute violations of system security. (SOURCE: CNSSI-4009)

**Threat Source:**

The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with Threat Agent. (SOURCE: FIPS 200; NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; CNSSI-4009)

**Timestamp:**

A sequence of characters or encoded information identifying when a certain event occurred, usually giving date and time of day, sometimes accurate to a small fraction of a second. Typically refers to digital date and time information attached to digital data. (SOURCE: Wikipedia)

**Token:**

Something that the claimant possesses and controls (typically a key or password) that is used to authenticate the Claimant's identity. (SOURCE: NIST SP 800-63)

Something that the claimant possesses and controls (such as a key or password) that is used to authenticate a claim. See also Cryptographic Token. (SOURCE: CNSSI-4009)

**Total Risk:**

The potential for the occurrence of an adverse event if no mitigating action is taken (i.e., the potential for any applicable threat to exploit a system vulnerability). (SOURCE: NIST SP 800-16)

**Tracking Cookie:**

A cookie placed on a user's computer to track the user's activity on different Web sites, creating a detailed profile of the user's behavior. (SOURCE: NIST SP 800-83)

**Traffic Analysis:**

A form of passive attack in which an intruder observes information about calls (although not necessarily the contents of the messages) and makes inferences, e.g., from the source and destination numbers, or frequency and length of the messages. (SOURCE: NIST SP 800-24)

The analysis of patterns in communications for the purpose of gaining intelligence about a system or its users. It does not require examination of the content of the communications, which may or may not be decipherable. For example, an adversary may be able to detect a signal from a reader that could enable it to infer that a particular activity is occurring (e.g., a shipment has arrived, someone is entering a facility) without necessarily learning an identifier or associated data. (SOURCE: NIST SP 800-98)

Gaining knowledge of information by inference from observable characteristics of a data flow, even if the information is not directly available (e.g., when the data is encrypted). These characteristics include the identities and locations of the (SOURCE(s) and destination(s) of the flow, and the flow's presence, amount, frequency, and duration of occurrence. (SOURCE: CNSSI-4009)

**Transmission Security – (TRANSEC):**

Measures (security controls) applied to transmissions in order to prevent interception, disruption of reception, communications deception, and/or derivation of intelligence by analysis of transmission characteristics such as signal parameters or message externals.

Note: TRANSEC is that field of COMSEC that deals with the security of communication transmissions, rather than that of the information being communicated. (SOURCE: CNSSI-4009)

**Transport Layer Security (TLS):**

An authentication and security protocol widely implemented in browsers and Web servers. (SOURCE: NIST SP 800-63)

**Trap Door:**

A means of reading cryptographically protected information by the use of private knowledge of weaknesses in the cryptographic algorithm used to protect the data.

In cryptography, one-to-one function that is easy to compute in one direction, yet believed to be difficult to invert without special information. (SOURCE: CNSSI-4009)

**Trojan Horse:**

A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. (SOURCE: CNSSI-4009)

**Trust Anchor:**

A public key and the name of a certification authority that is used to validate the first certificate in a sequence of certificates. The trust anchor's public key is used to verify the signature on a certificate issued by a trust anchor certification authority. The security of the validation process depends upon the authenticity and integrity of the trust anchor. Trust anchors are often distributed as self-signed certificates. (SOURCE: NIST SP 800-57 Part 1)

An established point of trust (usually based on the authority of some person, office, or organization) from which an entity begins the validation of an authorized process or authorized (signed) package. A "trust anchor" is sometimes defined as just a public key used for different purposes (e.g., validating a Certification Authority, validating a signed software package or key, validating the process [or person] loading the signed software or key). (SOURCE: CNSSI-4009)

A public or symmetric key that is trusted because it is directly built into hardware or software, or securely provisioned via out-of-band means, rather than because it is vouched for by another trusted entity (e.g. in a public key certificate). (SOURCE: NIST SP 800-63)

**Trusted Agent:**

Entity authorized to act as a representative of an agency in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities. (SOURCE: NIST SP 800-32; CNSSI-4009)

**Trusted Computer System:**

A system that employs sufficient hardware and software assurance measures to allow its use for processing simultaneously a range of sensitive or classified information. (SOURCE: CNSSI-4009)

**Trustworthiness:**

The attribute of a person or organization that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities. (SOURCE: NIST SP 800-79; CNSSI-4009; NIST SP 800-39)

Security decisions with respect to extended investigations to determine and confirm qualifications, and suitability to perform specific tasks and responsibilities. (SOURCE: FIPS 201)

**Tunneling:**

Technology enabling one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network. (SOURCE: CNSSI-4009)

**Twitter:**

An online social networking and microblogging service that enables users to send and read short 140-character text messages, called "tweets". Registered users can read and post tweets, but unregistered users can only read them. Users access Twitter through the website interface, SMS, or mobile device app. (SOURCE: Wikipedia)

**Two Factor Authentication:**

An approach that provides unambiguous identification of users by means of the combination of two different components. These components may be something that the user knows, something that the user possesses or something that is inseparable from the user. (SOURCE: Wikipedia)

**Unauthorized Access:**

Occurs when a user, legitimate or unauthorized, accesses a resource that the user is not permitted to use. (SOURCE: FIPS 191)

Any access that violates the stated security policy. (SOURCE: CNSSI-4009)

**Unauthorized Disclosure:**

An event involving the exposure of information to entities not authorized access to the information. (SOURCE: NIST SP 800-57 Part 1; CNSSI-4009)

**Uniform Resource Locator (URL):**

A specific character string that constitutes a reference to a resource. In most web browsers, the URL of a web page is displayed on top inside an address bar. A URL is technically a type of uniform resource identifier (URI), but in many technical documents and verbal discussions, URL is often used as a synonym for URI. URLs are commonly used for web pages (http), but can also be used for file transfer (ftp), email (mailto) and many other applications. (SOURCE: Wikipedia)

**Untrusted Process:**

Process that has not been evaluated or examined for correctness and adherence to the security policy. It may include incorrect or malicious code that attempts to circumvent the security mechanisms. (SOURCE: CNSSI-4009)

**User:**

The term “user” refers to any Executive Branch agency full-time or part-time employee, temporary worker, volunteer, intern, contractor, and those employed by contracted entities, who are provided authorized access to State information assets.  
(State of New Jersey Statewide Information Security Manual)

Individual or (system) process authorized to access an information system. (SOURCE: FIPS 200)

Individual, or (system) process acting on behalf of an individual, authorized to access an information system. (SOURCE: NIST SP 800-53; NIST SP 800-18; CNSSI-4009)

An individual or a process (subject) acting on behalf of the individual that accesses a cryptographic module in order to obtain cryptographic services. (SOURCE: FIPS 140-2)

**User Datagram Protocol (UDP):**

One of the core members of the Internet protocol suite. With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without prior communications to set up special transmission channels or data paths.  
(SOURCE: Wikipedia)

**User-ID:**

Unique symbol or character string used by an information system to identify a specific user.  
(SOURCE: CNSSI-4009)

**Validation:**

The process of demonstrating that the system under consideration meets in all respects the specification of that system. (SOURCE: FIPS 201)

Confirmation (through the provision of strong, sound, objective evidence) that requirements for a specific intended use or application have been fulfilled (e.g., a trustworthy credential has been presented, or data or information has been formatted in accordance with a defined set of rules, or a specific process has demonstrated that an entity under consideration meets, in all respects, its defined attributes or requirements). (SOURCE: CNSSI-4009)

**Vendor:**

A vendor, or a supplier, is a supply chain management term that means anyone who provides goods or services to a company or individuals. A vendor often manufactures inventoriable items and then sells those items to a customer. (SOURCE: Wikipedia)

**Verification:**

Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity’s requirements have been correctly defined, or an entity’s attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome). (SOURCE: CNSSI-4009)

**Virtual LAN (VLAN):**

In computer networking, a single layer-2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them via one or more routers; such a domain is referred to as a virtual local area network, virtual LAN or VLAN. (SOURCE: Wikipedia)

**Virtual Machine (VM):**

Software that allows a single host to run one or more guest operating systems. (SOURCE: NIST SP 800-115)

**Virtual Private Cloud (VPC):**

An on-demand configurable pool of shared computing resources allocated within a public cloud environment, providing a certain level of isolation between the different organizations (denoted as users hereafter) using the resources. (SOURCE: Cloud Security Alliance)

**Virtual Private Network (VPN):**

VPNs extend a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryptions. (SOURCE: Wikipedia)

**Virtualization:**

Refers to the logical abstraction of computing resources from physical constraints. One common abstraction is referred to as virtual machines or VMs, which takes the content of a physical machine and allows it to operate on different physical hardware and/or along with other virtual machines on the same physical hardware. In addition to VMs, virtualization can be performed on many other computing resources, including applications, desktops, networks, and storage. (SOURCE: PCI DSS GLOSSARY)

The simulation of the software and/or hardware upon which other software runs. This simulated environment is called a virtual machine (VM). (SOURCE: NIST)

**Virus:**

A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use email programs to spread itself to other computers, or even erase everything on a hard disk. (SOURCE: CNSSI-4009)

**Voice over IP (VoIP):**

A methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. Other terms commonly associated with VoIP are IP telephony, Internet telephony, voice over broadband

(VoBB), broadband telephony, IP communications, and broadband phone service. (SOURCE: Wikipedia)

**Vulnerability:**

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

(SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; NIST SP 800-60; NIST SP 800-115; FIPS 200)

A weakness in a system, application, or network that is subject to exploitation or misuse.

(SOURCE: NIST SP 800-61)

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. (SOURCE: CNSSI-4009)

**Vulnerability Scan:**

An automated process to proactively identify security weaknesses in a network or individual system. (SOURCE: ISACA)

**Warm Site:**

An environmentally conditioned workspace that is partially equipped with information systems and telecommunications equipment to support relocated operations in the event of a significant disruption. (SOURCE: NIST SP 800-34)

Backup site that typically contains the data links and preconfigured equipment necessary to rapidly start operations, but does not contain live data. Thus, commencing operations at a warm site will (at a minimum) require the restoration of current data. (SOURCE: CNSSI-400)

**Web-Based Connection:**

The connection provides access to one or more applications through a single centralized interface, through a direct application access or portal architecture, typically a web-browser to a portal server located within the demilitarized zone (DMZ). This type of connection creates an area that serves as a boundary between two or more networks and isolates the information asset from the internal private network. (SOURCE: State of New Jersey Statewide Information Security Manual)

**Web Bug:**

A tiny image, invisible to a user, placed on Web pages in such a way to enable third parties to track use of Web servers and collect information about the user, including IP address, host name, browser type and version, operating system name and version, and cookies. (SOURCE: NIST SP 800-28)

**WiFi Protected Access (WPA):**

Security protocol created to secure wireless networks. WPA is the successor to WEP. WPA2 was also released as the next generation of WPA. (SOURCE: PCI DSS GLOSSARY)

**Wired Equivalent Privacy (WEP):**

A security protocol, specified in the IEEE 802.11 standard, that is designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN. WEP is no longer considered a viable encryption mechanism due to known weaknesses. (SOURCE: NIST SP 800-48)

**Workaround:**

Reducing or eliminating the impact of an incident or problem for which a full resolution is not yet available. (SOURCE: ITIL V3)

**Worm:**

A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself. See Malicious Code. (SOURCE: CNSSI-4009)

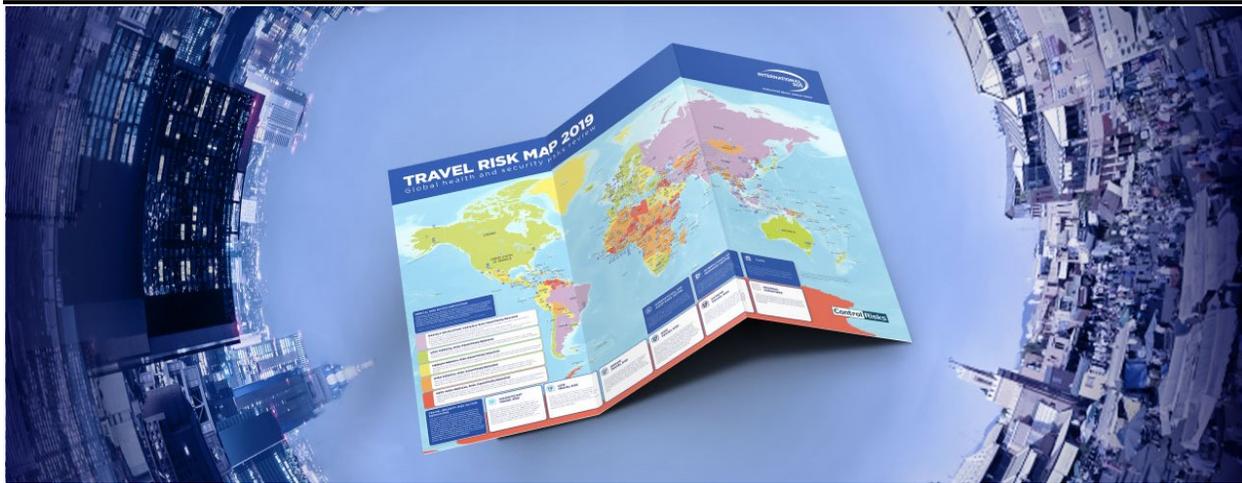
**Zeroization:**

A method of erasing electronically stored data, cryptographic keys, and CSPs by altering or deleting the contents of the data storage to prevent recovery of the data. (SOURCE: FIPS 140-2)

A method of erasing electronically stored data, cryptographic keys, and Credentials Service Providers (CSPs) by altering or deleting the contents of the data storage to prevent recovery of the data. (SOURCE: CNSSI)

---

## APPENDIX B – NJCCIC CYBERSECURITY GUIDELINES FOR INTERNATIONAL TRAVEL



While all travelers are subject to cybersecurity risks when traveling internationally, government officials and business travelers are considered high value targets due to their roles and the sensitivity of the information they may store or transmit. The NJCCIC recommends travelers and their organizations assess cyber risks based on the threats and vulnerabilities posed by the trip, the host jurisdiction, the traveler, and the traveler’s equipment and devices. The following guidelines are provided to assist the traveler and their organization in mitigating cyber risks presented by international travel.

### **Before You Go**

- As feasible, use electronic devices that your organization has procured and configured specifically for international travel.
- If you must take your electronic devices, make backup copies of all sensitive data and travel with only the absolute minimum necessary for your trip.
- Update your devices with the latest security patches, software updates, and anti-virus/anti-malware software.
- Disable your devices’ WiFi, Bluetooth, Near-Field Communications (NFC), and Location Services.
- Disable automatic logins, automatic network connections, auto-download features, and your devices’ USB ports.
- Enable multi-factor authentication, especially for all cloud services.
- Ensure your devices’ firewalls and all technical security controls are enabled.

- Familiarize yourself with your destination's laws as the use of encryption and some online behaviors are illegal in certain countries. Consult the [US State Department website](#) for information about particular destinations.
- If you are traveling on official New Jersey state government business, you must notify the New Jersey Office of Homeland Security and Preparedness at [notify@njohsp.gov](mailto:notify@njohsp.gov) prior to your trip.

## **While Traveling**

- Ensure the physical security of your devices at all times. Do not assume a hotel safe provides adequate protection. Keep your devices with you whenever possible.
- Do not connect to public or hotel WiFi networks. For data connectivity, use an assigned Mobile 4G Hotspot or Smartphone with an international data plan.
- Do not insert USB devices obtained or provided to you in the host country into your computer.
- As feasible and permissible by local laws, use encrypted connections such as a Virtual Private Network (VPN) to secure all data communications.
- Power off your devices when not in use.
- Do not use public charging stations for recharging USB-powered devices.
- Assume that all online activity is subject to government and/or other monitoring techniques.
- Report any suspicious activity or unexplained technical issues you experienced while traveling to your organization's information technology or security staff.

## **Upon Return**

- Do not connect your electronic devices to your personal or your organization's network until they have been scanned and/or reimaged by your information technology staff.
- Change all passwords used while traveling.

